RINGS OF INVARIANTS, F-REGULARITY, AND LOCAL COHOMOLOGY

by

Kenneth Carl Jeffries

A dissertation submitted to the faculty of
The University of Utah
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

The University of Utah

May 2015

The University of Utah Graduate School

STATEMENT OF DISSERTATION APPROVAL

The dissertation of **Kenneth Carl Jeffries**

has been approved by the following supervisory committee members:

Anurag K. Singh	, Chair	**3/11/2015** Date Approved
Tommaso de Fernex	, Member	**3/11/2015** Date Approved
Srikanth B. Iyengar	, Member	**3/11/2015** Date Approved
Lance E. Miller	, Member	**3/11/2015** Date Approved
Karl E. Schwede	, Member	**3/11/2015** Date Approved

and by **Peter E. Trapa** , Chair/Dean of

the Department/College/School of **Mathematics**

and by David B. Kieda, Dean of The Graduate School.

ABSTRACT

First, we recall some classical results from invariant theory, and the direct summand property of ring extensions. We review the local cohomology functors and the F-signature of a ring.

We consider the question of how many independent splittings the ring of invariants of a finite group action has; equivalently, what the F-signature of the invariant ring is. In particular, we consider the question of when the ring of invariants of a finite group G-action on a vector space over a field of positive characteristic $p > 0$, where p divides G, is a direct summand of the polynomial ring. We prove that if the a-invariant of the ring of invariants is equal to that of the polynomial ring, then it is not a direct summand. We provide further evidence for a conjecture of A. Broer related to this question.

Following the work of Watanabe–Yoshida, A. Singh, and M. Von Korff, we study the F-signature of affine toric varieties. We determine which affine toric varieties of a particular dimension have the largest F-signature, and analyze the structure of the set of values.

Next, we study the separating rank of a finite group action — the least number of invariants required to separate the orbits of the group action. We find a lower bound on the separating rank in terms of the ranks of generators of stabilizer subgroups of the action. This result is a generalization of a theorem of Serre on when rings of invariants are polynomial rings. We show that the lower bound is sharp for large classes of examples. This part is based on joint work with Emilie Dufresne.

We end by posing a question on the vanishing of local cohomology that implies a generalization of the Shephard–Todd theorem.

To David Flaspohler, from whom I learned the love of mathematics.

CONTENTS

ACKNOWLEDGEMENTS

I would like to thank my parents, Tim and Jenny, for their endless support and encouragement. My completion of this degree is their success above all else.

I also want to thank all my friends in Utah and in the Commutative Algebra community I have met along the way. They have made this experience so much fun, and have made it clear that I have found the right vocation.

Thanks are due to my collaborators. I have learned so much from the people I've worked with and enjoyed them all so much. Special thanks are due to Emilie Dufresne for allowing me to include joint work here.

I wish to recognize the department staff for maintaining such a pleasant and functional work environment. Many thanks, also, to the professors at The U and at The Ohio State from whom I've learned so much.

I have had many great opportunities to attend workshops and conferences in my time as a student. I thank the many people who have organized these conferences, as well as those who have funded me. Particular thanks on this account go to the NSF, to MSRI, and to Anurag and to Paul Roberts.

Thanks also to my committee for reading my dissertation, and for their individual roles in my development as a student.

Working with Anurag has been such a wonderful experience, and easily the best professional choice I have made in my career so far. Endless thanks are due to him for teaching me so much, for shaping my approach to mathematics and developing my interests, for leading me to so many interesting questions and suggesting so many fruitful approaches to them, for his unflagging optimism and patience, and for being such a great friend.

CHAPTER 1

INTRODUCTION

1.1 Group actions and invariant rings

We begin by reviewing the basic properties of rings of invariants of finite group actions, and setting notation. Proofs of the statements and theorems in this subsection can be found in [4].

Let $\Bbbk$ be a field, and V be a finite dimensional vector space over $\Bbbk$. A subgroup G of $\mathrm{GL}(V)$ comes naturally equipped with a linear action on the vector space V. The choice of an embedding of G into some $\mathrm{GL}(V)$ is equivalent to the choice of an abstract group and a representation of G on V.

Given a vector space V, the dual space V^* consists of all linear functions on V with values in $\Bbbk$, and the symmetric algebra $\mathrm{Sym}(V^*)$ can be thought of as the set of all polynomial functions on V. Indeed, a choice of basis $e_1^*, \ldots, e_n^*$ of V^* induces an isomorphism of $\Bbbk[V] := \mathrm{Sym}(V^*)$ with the polynomial ring $\Bbbk[x_1, \ldots, x_n]$ by sending e_i^* to x_i. The polynomial ring $\Bbbk[V]$ has Krull dimension equal to the dimension of V as a $\Bbbk$-vector space. By Hilbert's Nullstellensatz, if $\Bbbk$ is algebraically closed, then the maximal ideals of $\Bbbk[V]$ are in bijection with points of V: indeed, upon choosing coordinates for V (and hence a corresponding generating set for $\Bbbk[V]$) each maximal ideal can be written uniquely in the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, with $(a_1, \ldots, a_n) \in V$.

An action of G on V gives an action of G on V^* by setting $g(\ell) = \ell \circ g^{-1}$. This in turn extends to a degree-preserving action of G on $\Bbbk[V]$ as follows: extend the action to simple tensors by multiplication, and then extend to all of $\Bbbk[V]$ by linearity. This action sends homogeneous elements to homogeneous elements of the same degree.

It is worth noting that to give an action of G on V is equivalent to giving a degree-preserving action of G on a polynomial ring $R \cong \Bbbk[V]$: one recovers the action of G on V by taking the action of G on the space $[R]_1 \cong V^*$ of degree one forms, and taking the action on the dual vector space $V^{**} \cong V$. We will often describe G actions in this way.

The ring of invariants of the group action is

$$\Bbbk[V]^G := \{r \in \Bbbk[V] \mid g(r) = r \quad \text{for all} \quad g \in G\}.$$

This construction is useful from an algebraic point of view for providing many interesting examples of rings. It is also important from a geometric point of view, as, if G is finite, the ring $\Bbbk[V]^G$ gives the structure of a variety to the collection of orbits of G on V, when $\Bbbk$ is algebraically closed. To be precise, let ϕ be the bijection between $\operatorname{mSpec} \Bbbk[V]$ and V given above, and $i\colon \Bbbk[V]^G \hookrightarrow \Bbbk[V]$ the inclusion map. Then, there is a bijective map ψ such that the following diagram commutes

$$\begin{array}{ccc} \operatorname{mSpec} \Bbbk[V] & \xrightarrow[\sim]{\phi} & V \\ {\scriptstyle i^*}\downarrow & & \downarrow \\ \operatorname{mSpec} \Bbbk[V]^G & \xrightarrow{\psi} & V/G \end{array}, \tag{1.1}$$

where $V/G = \{G \cdot v \mid v \in V\}$ is the set of orbits, and the map from V to V/G sends v to its orbit $G \cdot v$.

Rings of invariants of finite group actions enjoy many nice properties. We list here some of the most basic ones.

Theorem 1.1. *Let G be a finite subgroup of $\mathrm{GL}(V)$.*

(1) $\Bbbk[V]^G$ is a graded, finitely generated $\Bbbk$-algebra.

(2) $\Bbbk[V]^G$ is a normal domain.

(3) The dimension of $\Bbbk[V]^G$ is equal to the dimension of V.

(4) $\Bbbk[V]$ is a finitely generated $\Bbbk[V]^G$-module of rank $|G|$.

1.2 Local cohomology

For the convenience of the reader unfamiliar with local cohomology, we give a quick review with an eye towards the main facts we will employ. Two welcoming sources on local cohomology which include the material below are [8, 25]. For an ideal I in a commutative noetherian ring R and an R-module M, the *I-torsion* part of M is

$$\Gamma_I(M) = \{m \in M \mid I^t m = 0 \text{ for some } t \in \mathbb{N}\}.$$

The assignment $\Gamma_I(-)$ is easily checked to be a left-exact functor from R-mod to itself (with maps given by restriction), and its right-derived functors are defined as the *local cohomology*

functors with support in I, denoted $\mathrm{H}^i_I(-)$. Since $\Gamma_I(-) = \Gamma_J(-)$ if $\sqrt{I} = \sqrt{J}$, we also have $\mathrm{H}^i_I(-) = \mathrm{H}^i_J(-)$.

Given a generating set $I = (f_1, \dots, f_t)$, the local cohomology with support in I can also be computed as the cohomology of the Čech complex:

$$\mathrm{H}^i_I(M) = \mathrm{H}^i \Big(\quad 0 \to M \to \bigoplus_j M_{f_j} \to \bigoplus_{j<j'} M_{f_j f_{j'}} \to \cdots \to M_{f_1 \cdots f_t} \to 0 \quad \Big) \,,$$

where the maps on each component are ± 1 times the natural maps, with the signs chosen so that the sequence above forms a complex. Consequently, if $\mathrm{H}^i_I(R) \neq 0$ and $f_1, \dots, f_t$ generates I up to radical, we necessarily have $t \geqslant i$, since the Čech complex must have at least i terms if its i^{th} cohomology is nonzero.

From the characterization of local cohomology in terms of Čech cohomology, it is readily apparent that the calculation of local cohomology is independent of the base ring. More precisely, if S is an R-algebra, I is an ideal of R, and M is an S-module, then $\mathrm{H}^i_{IS}(M)|_R$ is canonically isomorphic to $\mathrm{H}^i_I(M|_R)$, where $(-)|_R$ is restriction of scalars.

If $(R, \mathfrak{m}, \Bbbk)$ is a local ring — a noetherian ring R with a unique maximal ideal $\mathfrak{m}$ and residue field $R/\mathfrak{m} = \Bbbk$ — the local cohomology with support in the maximal ideal contains much information about the structural qualities of the ring. In particular, the depth of R is the least i for which $\mathrm{H}^i_{\mathfrak{m}}(R) \neq 0$ and the dimension of R is the maximum such i. In particular, R is Cohen-Macaulay if and only if $\mathrm{H}^i_{\mathfrak{m}}(R) \neq 0$ only for $i = \dim R$.

We recall that a canonical module of a local ring $(R, \mathfrak{m}, \Bbbk)$ is a finitely generated module M whose Matlis dual $\mathrm{Hom}_R(M, E_R(\Bbbk))$ is isomorphic to the top local cohomology of R with support in $\mathfrak{m}$. For a graded ring, the canonical module is a module whose graded dual $\underline{\mathrm{Hom}}_R(M, \Bbbk)$ has a degree-preserving isomorphism with the top local cohomology of R. For a polynomial ring R in n variables, each with degree one, $R(n)$ is a canonical module. We denote a canonical module of R by ω_R.

If S is an R-algebra that is a finite module over R, a canonical module of S is related to that of R by the following formula:

$$\omega_S \cong \mathrm{Ext}_R^{\dim R - \dim S}(S, \omega_R) \,;$$

in the graded case one has the exact analogue

$$\omega_S \cong \underline{\mathrm{Ext}}_R^{\dim R - \dim S}(S, \omega_R) \,.$$

In particular, if R is a subring of S and the extension $R \subseteq S$ is module-finite, then

$$\omega_S \cong \mathrm{Hom}_R(S, \omega_R) \,,$$

and in the graded case,

$$\omega_S \cong \underline{\mathrm{Hom}}_R(S, \omega_R)\,.$$

For a graded ring R of dimension n, not necessarily either Cohen-Macaulay or standard graded, we define the *a-invariant* of R to be the largest integer t such that $[\mathrm{H}^n_{\mathfrak{m}}(R)]_t \neq 0$. Equivalently, the a-invariant is the negative of the smallest integer s such that $[\omega_R]_s \neq 0$.

1.3 F-regularity and F-signature

Let R be a ring of prime characteristic $p > 0$. The Frobenius map F on R is the endomorphism of R sending any element to its p^{th} power. If R is reduced, the Frobenius map is injective, and hence R is isomorphic to its image under the map. In the case that R is a domain, R as an R-module with structure given by restriction of scalars via F can be identified with the ring $R^{1/p}$ of p^{th} roots of R inside an algebraic closure of its fraction field, where the module structure on $R^{1/p}$ comes from the natural inclusion. Similarly, the R-module structure on R given by restriction of scalars via F^e is the same as the natural module structure on R^{1/p^e}.

Definition 1.1. (Hochster–Huneke). *A domain R of characteristic $p > 0$ is* strongly F-regular *if for any $c \in R$, there exists some integer e and an R-linear map $\phi : R^{1/p^e} \to R$ such that*

1. *$\phi \circ i = 1 : R \to R$, where $i : R \to R^{1/p^e}$ is the inclusion, and*
2. *$\phi(c^{1/p^e}) = 1$.*

The strong F-regularity property has some important connections with the direct summand property.

Theorem 1.2. (Hochster–Huneke [23]). *Let $R \subseteq S$ be domains of characteristic $p > 0$.*

1. *If S is strongly F-regular and R is a direct summand of S as an R-module, then R is strongly F-regular.*
2. *If R is strongly F-regular, and S is a finite R-module, then R is a direct summand of S as an R-module.*

We note also the following important consequence of the strong F-regularity property.

Theorem 1.3. (Hochster–Huneke [23]). *If R is strongly F-regular, then R is Cohen-Macaulay.*

Definition 1.2. (Huneke–Leuschke, Smith–Van den Bergh [24, 39]). *Let $(R, \mathfrak{m}, \Bbbk)$ be a local or graded domain of characteristic $p > 0$ and dimension d. Suppose that $\Bbbk$ is a finite extension of $\Bbbk^p$. For each $e > 0$, let a_e be the maximal rank of a free summand of R^{1/p^e} as an R-module. Then the limit*

$$s(R) = \lim_{e\to\infty} \frac{a_e}{([\Bbbk : \Bbbk^p]p^d)^e}$$

is called the F-signature of R.

It is a theorem, due to Tucker [42], that the limit above exists.

The F-signature takes values between 0 and 1, and it is 1 if and only if R is regular, as established in [24]. By a theorem of Aberbach and Leuschke [1], the F-signature of R is nonzero if and only if R is strongly F-regular. In this way, this is a numerical invariant that measures how far R is from being regular.

Proposition 1.4. ([24]). *Let $R \subseteq S$ be domains of characteristic $p > 0$, and S be regular. If f is the maximal rank of a free R-summand of S, and h is the rank of S as an R-module, then the F-signature of R is $s(R) = \dfrac{f}{h}$.*

We will also consider three notions related to strong F-regularity.

Definition 1.3. *Let R be a noetherian ring of prime characteristic $p > 0$.*

1. *R is F-rational if every parameter ideal of R is tightly closed. That is, for every parameter ideal I, $r \notin I$, and $c \in R$, for each $e \in \mathbb{N}$, $cr^{p^e} \notin I^{[p^e]}$.*

2. *R is F-pure if the Frobenius map is a pure morphism.*

3. *R is F-injective if every parameter ideal is Frobenius closed. That is, for every parameter ideal I, and $r \notin I$, for each $e \in \mathbb{N}$, $r^{p^e} \notin I^{[p^e]}$.*

In general, strongly F-regular implies F-rational and F-pure, and F-rational and F-pure each imply F-injective. If R is Gorenstein, then strongly F-regular and F-rational are equivalent, and F-pure and F-injective are equivalent.

1.4 Classical results

A general question in invariant theory is to determine when the ring of invariants of a group action has some favorable algebraic property in terms of the geometry of the group action. We collect here a few such results.

Definition 1.4. *Let G be a subgroup of* $\mathrm{GL}(V)$*. An element $g \in G$ is a* pseudoreflection *if the rank of $1 - g$ as a $\Bbbk$-linear endomorphism of V is less than or equal to one.*

Theorem 1.5. (Chevalley, Shephard–Todd, Serre, Clark–Ewing [11, 12, 34, 36]). *Let G be a finite subgroup of* $\mathrm{GL}(V)$ *and suppose that $|G|$ is not divisible by the characteristic of $\Bbbk$. Then $\Bbbk[V]^G$ is a polynomial ring if and only if G is generated by pseudoreflections.*

Example 1.6. Let $\mathcal{S}_n$ be the symmetric group on n letters, $V = \Bbbk^n$, with $\operatorname{char} \Bbbk > n$, and embed $\mathcal{S}_n$ in $\mathrm{GL}(V)$ so that $\mathcal{S}_n$ acts by permuting coordinates. The transposition (12) is given by the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix},$$

which is similar to

$$\begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix};$$

likewise, any 2-cycle is a pseudoreflection, so $\mathcal{S}_n$ is generated by psuedoreflections. As guaranteed by the Shephard-Todd theorem, $\Bbbk[V]^{\mathcal{S}_n} = \Bbbk[e_1, \ldots, e_n]$ is a polynomial ring, generated by the elementary symmetric functions.

Now let $\mathcal{A}_n \subset \mathcal{S}_n$ be the alternating group. The alternating group contains no 2-cycles; a generating set is given by 3-cycles. For example, the 3-cycle (123) is given by the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix},$$

which is similar to

$$\begin{bmatrix} \omega^2 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix};$$

over a field with a primitive cube root of unity ω. The group $\mathcal{A}_n$ is not generated by pseudoreflections, and its ring of invariants is $\Bbbk[V]^{\mathcal{A}_n} = k[e_1, \ldots, e_n, \Delta]$, where

$$\Delta = \prod_{i<j}(x_i - x_j)\,,$$

and thus it is not a polynomial ring. We will examine the ring of invariants of this action further in Example 2.21.

If the hypothesis in Theorem 1.5 on the order of G is dropped, then one direction of the theorem still holds. In fact, there is a strengthened form, due to Serre.

Theorem 1.7. (Serre [34]). *Let G be a finite subgroup of $GL(V)$. If $\Bbbk[V]^G$ is a polynomial ring, then for every vector subspace W of V, the stabilizer subgroup of W is generated by pseudoreflections.*

It was conjectured by Kac [26] that the converse to this statement holds. However, the following example shows that this is not the case.

Example 1.8. (Campbell–Hughes–Shank [9]). Let $\Bbbk$ be a field of characteristic $p > 0$ and let $G = \langle \alpha, \beta, \gamma \rangle \cong (\mathbb{Z}/p)^3$ act on $R = \Bbbk[x_1, x_2, y_1, y_2]$ by

$$\alpha(x_i) = \beta(x_i) = \gamma(x_i) = x_i \qquad \text{for } i = 1, 2\,,$$

$$\alpha \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 + x_1 \\ y_2 \end{pmatrix}, \quad \beta \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 + x_2 \end{pmatrix},$$
$$\gamma \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 + x_1 + x_2 \\ y_2 + x_1 + x_2 \end{pmatrix}.$$

One can verify that for every vector subspace W of V, the stabilizer subgroup of W is generated by pseudoreflections. The ring of invariants is

$$\Bbbk[V]^G = \Bbbk\Big[x_1, x_2, x_1 \prod_{g\in\langle\alpha\rangle} g(y_1) + x_2 \prod_{g\in\langle\beta\rangle} g(y_2),\ \prod_{g\in\langle\alpha,\gamma\rangle} g(y_1),\ \prod_{g\in\langle\alpha,\gamma\rangle} g(y_2)\Big]$$
$$= \frac{\Bbbk\big[x_1, x_2, w, z_1, z_2\big]}{\Big(w^p - x_1^p z_1 - x_2^p z_2 - w\big(\sum_{j=1}^{p}(x_1^{p-j+1}x_2^j)^{p-1}\big)\Big)};$$

specifically, it is a hypersurface.

One important tool in the study of invariants of finite groups is the *trace* or *transfer* map $\operatorname{Tr}^G : \Bbbk[V] \to \Bbbk[V]^G$ given by

$$\operatorname{Tr}^G(r) = \sum_{g\in G} g(r)\,.$$

Much of its importance comes from the fact that, when $|G|$ is a unit, the map $\dfrac{1}{|G|}\operatorname{Tr}^G$ is a $\Bbbk[V]^G$-linear splitting of the inclusion map $i : \Bbbk[V]^G \to \Bbbk[V]$; that is, the following diagram commutes:

$$\begin{array}{ccc} \Bbbk[V]^G & \xrightarrow{\quad 1 \quad} & \Bbbk[V]^G \\ & {\scriptstyle i}\searrow \quad \nearrow{\scriptstyle |G|^{-1}\operatorname{Tr}^G} & \\ & \Bbbk[V] & \end{array} \qquad (1.2)$$

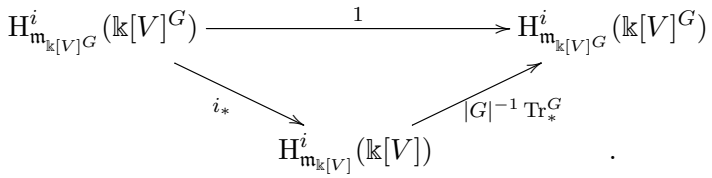
Thus, when $|G|$ is a unit, by Theorem 1.2, $\Bbbk[V]^G$ is strongly F-regular, and hence, by Theorem 1.3, $\Bbbk[V]^G$ is Cohen-Macaulay. With an eye towards questions we will consider later, we provide a more direct proof of the latter consequence.

Theorem 1.9. (Hochster–Eagon [22]). *Let G be a finite subgroup of $\mathrm{GL}(V)$ and suppose that $|G|$ is not divisible by the characteristic of $\Bbbk$. Then $\Bbbk[V]^G$ is Cohen-Macaulay.*

Proof. Apply the i^{th} local cohomology functor with support in the maximal ideal of $\Bbbk[V]^G$, $\mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]^G}}(-)$, to the triangle (1.2) above to obtain:

$$\begin{array}{ccc} \mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]^G}}(\Bbbk[V]^G) & \xrightarrow{\quad 1 \quad} & \mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]^G}}(\Bbbk[V]^G) \\ & {\scriptstyle i_*}\searrow \quad \nearrow{\scriptstyle |G|^{-1}\operatorname{Tr}^G_*} & \\ & \mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]^G}}(\Bbbk[V]) & \end{array}\,.$$

Since the radical of $\mathfrak{m}_{\Bbbk[V]^G}$ in $\Bbbk[V]$ is $\mathfrak{m}_{\Bbbk[V]}$, we have that $\mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]^G}}(\Bbbk[V]) \cong \mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]}}(\Bbbk[V])$, so the following commutes for all i:



Therefore the map $i_* : \mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]^G}}(\Bbbk[V]^G) \to \mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]}}(\Bbbk[V])$ is injective. However, $\Bbbk[V]$ is Cohen-Macaulay, so $\mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]}}(\Bbbk[V])$ is nonzero only for $i = \dim(V)$, hence $\mathrm{H}^i_{\mathfrak{m}_{\Bbbk[V]^G}}(\Bbbk[V]^G)$ is nonzero only for $i = \dim(V)$, and thus $\Bbbk[V]^G$ is Cohen-Macaulay. ∎

As with the Shephard-Todd theorem, the Hochster-Eagon theorem fails when the hypothesis on the characteristic of $\Bbbk$ is dropped. The following example is well-known:

Example 1.10. Let $G = \langle\sigma\rangle \cong \mathbb{Z}/2$ act on $\Bbbk[V] = \mathbb{F}_2[x_1, y_1, x_2, y_2, x_3, y_3]$ by:

$$\sigma(x_i) = y_i \qquad \text{for } i = 1, 2, 3\,,$$

$$\sigma(y_i) = x_i \qquad \text{for } i = 1, 2, 3\,.$$

Then the ring of invariants

$$\begin{aligned}\Bbbk[V]^G = \mathbb{F}_2[&x_1 + y_1, x_2 + y_2, x_3 + y_3, x_1y_1, x_2y_2, x_3y_3,\\ &x_1y_2 + x_2y_1, x_1y_3 + x_3y_1, x_2y_3 + x_3y_2, x_1x_2x_3 + y_1y_2y_3]\end{aligned}$$

is not Cohen-Macaulay. Indeed, $x_1 + y_1, x_2 + y_2, x_3 + y_3, x_1y_1, x_2y_2, x_3y_3$ is a system of parameters, and one has the relation

$$(x_1 + y_1)(x_2y_3 + x_3y_2) + (x_2 + y_2)(x_1y_3 + x_3y_1) + (x_3 + y_3)(x_1y_2 + x_2y_1) = 0\,,$$

in $\Bbbk[V]^G$, so that $x_3 + y_3$ is a zerodivisor in $\Bbbk[V]^G/(x_1 + y_1, x_2 + y_2)$, and hence, the ring of invariants is not Cohen-Macaulay.

The following example of Bertin [5] is historically the first example of a unique factorization domain that is not Cohen-Macaulay.

Example 1.11. (Bertin). Let $G = \langle\alpha\rangle \cong \mathbb{Z}/4$ act on $\mathbb{F}_2[x_1, x_2, x_3, x_4]$ by cyclically permuting coordinates:

$$\alpha(x_i) = x_{i+1} \quad \text{for } i = 1, 2, 3, \qquad \alpha(x_4) = x_1\,.$$

Then the ring of invariants

$$\begin{aligned}\Bbbk[V]^G =&\mathbb{F}_2\Big[\operatorname{Tr}^G(x_1), \operatorname{Tr}^G(x_1x_2), \frac{1}{2}\operatorname{Tr}^G(x_1x_3), \operatorname{Tr}^G(x_1x_2x_3), \operatorname{Tr}^G(x_1^2x_3x_4) + \frac{1}{2}\operatorname{Tr}^G(x_1^2x_3^2),\\ &\operatorname{Tr}^G(x_1^2(x_3+x_4)), x_1x_2x_3x_4, \operatorname{Tr}^G(x_1^2(x_1+x_2)x_3x_4 + x_1^2x_2^2(x_3+x_4) + x_1^2x_2x_3^2)\Big]\end{aligned}$$

is not Cohen-Macaulay.

The theorems and examples in this section illustrate the general theme that the properties of the ring of invariants of a group $\Bbbk[V]^G$ are related to the action of the group G, but it is harder to ensure good properties of $\Bbbk[V]^G$ in the case when the order of the group is not invertible. As this hypothesis plays a key role in the invariant theory of finite groups, we say that the action in *nonmodular* if $|G|$ is a unit in $\Bbbk$ and *modular* otherwise.

CHAPTER 2

SPLITTINGS FOR INVARIANT RINGS OF FINITE GROUPS

2.1 Introduction

Throughout this chapter, we consider a finite subgroup G of $\mathrm{GL}(V)$ with its natural action on a $\Bbbk$-vector space V and the polynomial ring $\Bbbk[V]$. As illustrated in the Introduction, the property that $\Bbbk[V]^G$ is a direct summand of $\Bbbk[V]$ is of great importance for $\Bbbk[V]^G$ having good properties. The Reynolds map $\frac{1}{|G|}\operatorname{Tr}^G$ provides a splitting of the inclusion in the nonmodular case; in the modular case, there may or may not exist splittings: e.g., in Example 1.11, the ring of invariants is not Cohen-Macaulay, so we see from the proof of Theorem 1.9 that $\Bbbk[V]^G$ cannot be a direct summand of $\Bbbk[V]$ as $\Bbbk[V]^G$-modules. In the nonmodular case, one may ask how many independent splittings exist. That is, what is the largest rank of a free $\Bbbk[V]^G$-summand of $\Bbbk[V]$?

When the characteristic of $\Bbbk$ is positive, these questions may be rephrased in terms of intrinsic properties of $\Bbbk[V]^G$. By Proposition 1.4 and Theorem 1.1 (4), the F-signature of $\Bbbk[V]^G$ is equal to the largest rank of a free $\Bbbk[V]^G$-submodule of $\Bbbk[V]$ divided by the order of the group. By Theorem 1.2, the ring of invariants is strongly F-regular if and only if the inclusion of $\Bbbk[V]^G$ into $\Bbbk[V]$ splits as $\Bbbk[V]^G$-modules. We thus ask the questions (equivalent to those above) what is the F-signature of $\Bbbk[V]^G$ and, in the modular case, when is $\Bbbk[V]^G$ strongly F-regular?

The first question is considered in Huneke–Leuschke [24], where it is shown for the simple A_n, D_n, and E_n singularities that the F-signature is equal to the reciprocal of the order of the group. The second question is considered by Glassbrenner [19], Singh [37], and Smith [40], who demonstrated that even Cohen-Macaulay rings of invariants, such as that of the alternating group $\mathcal{A}_n$, may fail to be strongly F-regular. This question is also considered by Broer [6, 7], who conjectured that if G is generated by pseudoreflections, $\Bbbk[V]^G$ is a direct summand of $\Bbbk[V]$ if and only if $\Bbbk[V]^G$ is in fact a polynomial ring.

In Section 2.2, we determine the maximal rank of a free $\Bbbk[V]^G$-summand of $\Bbbk[V]$ in the nonmodular case. Consequently, we give a formula for the F-signature of $\Bbbk[V]^G$ in terms of the G-action alone. In Section 2.3, we consider the question of when $\Bbbk[V]^G$ is a direct summand of $\Bbbk[V]$ — equivalently, when $\Bbbk[V]^G$ is strongly F-regular — in the case of representations of $\mathbb{Z}/p\mathbb{Z}$ over a field of characteristic p. In Section 2.4, we give a necessary condition for the inclusion $\Bbbk[V]^G \subseteq \Bbbk[V]$ to split, that generalizes the example of the alternating group $\mathcal{A}_n$.

2.2 Splittings for nonmodular actions

Definition 2.1. *Let S be a ring, and H a group equipped with an action on S. The* skew group ring*, denoted as $S\#H$, is a free S-module with basis the elements of H, and multiplication*

$$s_1h_1 \cdot s_2h_2 = s_1h_1(s_2)\, h_1h_2\,.$$

Theorem 2.1. (Auslander [3]). *If G has no pseudoreflections other than the identity, then $\mathrm{End}_{\Bbbk[V]^G}(\Bbbk[V]) \cong \Bbbk[V]\#G$ via the natural map sending $r \in \Bbbk[V]$ to multiplication by r and g to its representation on $\Bbbk[V]$.*

We abuse notation by identifying elements $g \in G$ and $t \in \Bbbk[V]$ with the associated maps in $\mathrm{End}_{\Bbbk[V]^G}(\Bbbk[V])$, or the restriction of such a map to $\Bbbk[V]^G$. No confusion should occur.

Lemma 2.2. *Let G be a finite nonmodular subgroup of $\mathrm{GL}(V)$. Let H be the subgroup of G generated by pseudoreflections.*

(a) The subgroup H is normal in G.

(b) The induced action of G/H on $\Bbbk[V]^H$ contains no pseudoreflections other than the identity.

Proof. (a) It suffices to show that a conjugate of a pseudoreflection in G is also a pseudoreflection, which is immediate from the definition.
(b) By hypothesis, Theorem 1.5 applies to $\Bbbk[V]^H$, so that one has a well-defined notion of pseudoreflection in the action of G/H on $\Bbbk[V]^H$. If $\bar{g}$ acts as a pseudoreflection in the induced action on $\Bbbk[V]^H$, then

$$\left(\Bbbk[V]^H\right)^{\langle \bar{g} \rangle} = \Bbbk[V]^{\langle H, g \rangle}$$

is a polynomial ring; so, by Theorem 1.5, $\langle H, g\rangle$ is generated by pseudoreflections. Thus, $g \in H$, so no nontrivial element of G/H is a pseudoreflection. ∎

Theorem 2.3. *Let G be a finite nonmodular subgroup of* $\mathrm{GL}(V)$*. Let H be the subgroup of G generated by pseudoreflections.*

(1) If G contains no pseudoreflections, then the maximal rank of a free $\Bbbk[V]^G$-summand of $\Bbbk[V]$ is one.

(2) More generally, the maximal rank of a free $\Bbbk[V]^G$-summand of $\Bbbk[V]$ is equal to the order of H.

Proof. (1) Let $t : \Bbbk[V]^G \hookrightarrow \Bbbk[V]$ denote the inclusion map determined by $1 \mapsto t \in \Bbbk[V]$. We will show that there is a $\Bbbk[V]^G$-linear retraction map $\rho : \Bbbk[V] \to \Bbbk[V]^G$ so that $\rho t = 1$, if and only if t is a unit. Given such a retraction, Theorem 2.1 ensures that $t\rho \in \mathrm{End}_{\Bbbk[V]^G}(\Bbbk[V])$ is given by an element $\sum_{g\in G} r_g g$ in $\Bbbk[V]\#G$. We check when the map $\rho = \displaystyle\sum_{g\in G} \frac{r_g}{t} g$ has image in $\Bbbk[V]^G$:

$$
\begin{aligned}
& h \sum_{g\in G} \frac{r_g}{t} g(s) = \sum_{g\in G} \frac{r_g}{t} g(s) && \forall h \in G,\, \forall s \in \Bbbk[V] \\
\iff \quad & \sum_{g\in G} h(\tfrac{r_g}{t}) hg(s) = \sum_{g\in G} \frac{r_g}{t} g(s) && \forall h \in G,\, \forall s \in \Bbbk[V] \\
\iff \quad & \sum_{g\in G} \frac{h(r_g)}{h(t)} hg(s) = \sum_{g\in G} \frac{r_g}{t} g(s) && \forall h \in G,\, \forall s \in \Bbbk[V] \\
\iff \quad & \sum_{g\in G} \frac{h(r_{h^{-1}g})}{h(t)} g(s) = \sum_{g\in G} \frac{r_g}{t} g(s) && \forall h \in G,\, \forall s \in \Bbbk[V] \\
\iff \quad & \frac{h(r_{h^{-1}g})}{h(t)} = \frac{r_g}{t} && \forall g, h \in G \\
\implies \quad & \frac{t}{g(t)} g(r_e) = r_g && \forall g \in G\,.
\end{aligned}
$$

Then,

$$1 = \rho t(1) = \sum_{g\in G} r_g g(t) = \sum_{g\in G} \frac{t}{g(t)} g(r_e) g(t) = \sum_{g\in G} t g(r_e)\,.$$

Since G acts by degree-preserving maps, we have $t \in \Bbbk$ as required. On the other hand, given $t \in \Bbbk$, the Reynolds map $\rho = \dfrac{t}{|G|}\,\mathrm{Tr}^G = \displaystyle\sum_{g\in G} \frac{t}{|G|} g$ is a retraction.

(2) Note that $\Bbbk[V]^G = (\Bbbk[V]^H)^{(G/H)}$. By Theorem 1.5, $\Bbbk[V]^H$ is a polynomial ring. Then, by Lemma 2.2, we may apply part (1) above. ∎

Example 2.4. Let $G = \langle \alpha, \beta \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/4$ act on $\mathbb{C}^3$ by

$$\alpha = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \beta = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & i \end{bmatrix}.$$

Note that the subgroup generated by pseudoreflections is $\langle\beta\rangle \cong \mathbb{Z}/4$. The ring of invariants is $\Bbbk[V]^G = \mathbb{C}[x^2, xy, y^2, z^4]$. As a $\Bbbk[V]^G$-module, $\Bbbk[V]$ has a direct sum decomposition

$$\begin{aligned}\Bbbk[V] =& 1 \cdot \Bbbk[V]^G \oplus z \cdot \Bbbk[V]^G \oplus z^2 \cdot \Bbbk[V]^G \oplus z^3 \cdot \Bbbk[V]^G \\ & \oplus (x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G) \oplus z(x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G) \\ & \oplus z^2(x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G) \oplus z^3(x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G).\end{aligned}$$

We claim that

$$\begin{aligned}M =& (x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G) \oplus z(x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G) \\ & \oplus z^2(x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G) \oplus z^3(x \cdot \Bbbk[V]^G + y \cdot \Bbbk[V]^G)\end{aligned}$$

has no free $\Bbbk[V]^G$-summand. Indeed, a free summand is generated by a minimal generator of the module, so is of the form

$$f = a_0x + b_0y + a_1xz + b_1yz + a_2xz^2 + b_2z^2 + a_3xz^3 + b_3yz^3.$$

We may write

$$xyf = x^2(a_0y + a_1yz + a_2yz^2 + a_3yz^3) + y^2(b_0x + b_1xz + b_2xz^2 + b_3xz^3). \tag{2.1}$$

If $f \neq 0$, then $a_0y + a_1yz + a_2yz^2 + a_3yz^3$ and $b_0x + b_1xz + b_2xz^2 + b_3xz^3$ are minimal generators of M that are not nonzero elements of $\Bbbk \cdot f$, so are in the kernel of the retraction associated to the inclusion. Thus, the right-hand side of (2.1) goes to zero under the associated retraction, contradiction the existence of such f. Consequently, the free part has rank four, which is equal to the order of the subgroup generated by pseudoreflections.

By Lemma 1.4, if f is the maximal rank of a free $\Bbbk[V]^G$-summand of R, then the F-signature of $\Bbbk[V]^G$ is $s(\Bbbk[V]^G) = \dfrac{f}{|G|}$. Thus, we have the following.

Corollary 2.5. *The F-signature of $\Bbbk[V]^G$ is $s(\Bbbk[V]^G) = \dfrac{|H|}{|G|}$.*

2.3 Invariants of modular representations of $\mathbb{Z}/p\mathbb{Z}$

Proposition 2.6. *Any representation of $\mathbb{Z}/p\mathbb{Z}$ over a field of positive prime characteristic p can be expressed as a direct sum of representations of the form $\mathbf{V}_n$ for $1 \leqslant n \leqslant p$, where $\mathbf{V}_n$ is the n-dimensional representation in which a generator for $\mathbb{Z}/p\mathbb{Z}$ acts on a basis via the Jordan block*

$$\mathbf{J}_n = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Proof. Write σ for a generator or $\mathbb{Z}/p\mathbb{Z}$. We then have $\sigma^p = 1$, so $(\sigma - 1)^p = 0$, and the unique eigenvalue of σ is 1 with multiplicity n. Note that this forces the inequality $n \leqslant p$. In particular, the eigenvalues lie in $\mathbb{F}_p$, hence, in the field of the representation. We can then realize σ as a block Jordan matrix:

$$\left[\begin{array}{c|c|c|c} \mathbf{J}_{n_1} & \mathbf{0} & \dots & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{J}_{n_2} & \dots & \mathbf{0} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathbf{0} & \mathbf{0} & \dots & \mathbf{J}_{n_k} \end{array}\right].$$

Thus, the representation is a direct sum of $\mathbf{V}_{n_i}$ with $n_i \leqslant p$. ∎

One can verify by induction that powers of the n-dimensional such a Jordan block are

$$(\mathbf{J}_n)^m = \begin{bmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{n-2} & \binom{m}{n-1} \\ 0 & 1 & \binom{m}{1} & \cdots & \binom{m}{n-3} & \binom{m}{n-2} \\ 0 & 0 & 1 & \cdots & \binom{m}{n-4} & \binom{m}{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{m}{1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Definition 2.7. Let G be a finite subgroup of $\mathrm{GL}_n(\Bbbk)$. An element $g \in G$ is said to be a *bireflection* if $\operatorname{rank}(1 - g) \leqslant 2$.

Theorem 2.8. (Kemper [27]). *Let P be a finite subgroup of $\mathrm{GL}(V)$ of order p^e, with $\Bbbk$ a field of characteristic p. If the invariant subring $\Bbbk[V]^P$ is Cohen-Macaulay, then P is generated by bireflections.*

Since any strongly F-regular ring is Cohen-Macaulay, we will consider representations of $\mathbb{Z}/p$ generated by a bireflection, and determine which are strongly F-regular.

Example 2.9. Consider the representation $\mathbf{V}_2 \oplus \mathbf{V}_2$ of $C = \mathbb{Z}/p\mathbb{Z}$. The ring of invariants of $\Bbbk[V] = \Bbbk[x_1, y_1, x_2, y_2]$ is

$$\Bbbk[V]^C = \Bbbk[x_1^p - y_1^{p-1}x_1, y_1, x_2^p - y_2^{p-1}x_2, y_2, x_1y_2 - x_2y_1] \cong \frac{\Bbbk[x, y, u, v, z]}{(z^p - x^{p-1}y^{p-1}z - ux^p - vy^p)}\,.$$

Since $\Bbbk[V]^C$ is a hypersurface, it is Gorenstein and in particular Cohen-Macaulay. We will show that $\Bbbk[V]^C$ is not F-injective if $p \geqslant 3$. Note that $I = (x, y, u, v)$ is a parameter ideal, with respect to which z^{p-1} is a socle generator. We then have

$$z^p \equiv (xy)^{p-1}z \bmod (x^p, y^p)\,,$$

so if $p \geqslant 3$, whence $2p - 2 \geqslant p$, also,

$$\begin{aligned} z^{(p-1)p} &\equiv (z^p)^2 z^{(p-3)p} \bmod (x^p, y^p) \\ &\equiv (xy)^{2p-2} z^{(p-3)p+2} \bmod (x^p, y^p) \\ &\equiv 0 \bmod (x^p, y^p)\,. \end{aligned}$$

Thus z^{p-1} lies in the Frobenius closure of I, but not in I itself, so $\Bbbk[V]^C$ is not F-injective.

Example 2.10. Consider the representation $\mathbf{V}_3$ of $C = \mathbb{Z}/p\mathbb{Z}$, where p is odd. The ring of invariants of $\Bbbk[V] = \Bbbk[x, y, z]$ is

$$\Bbbk[V]^C = K[z, y^p - z^{p-1}y, N(x), y^2 - 2xz - yz]\,,$$

where $N(x) = \prod_{\sigma \in C} \sigma(x)$. Again, the ring of invariants is a hypersurface, hence Gorenstein.

We claim that $\Bbbk[V]^C$ is not F-injective if $p \geqslant 5$. Note that

$$I = (z, y^p - z^{p-1}y, N(x))$$

is a parameter ideal. First, we argue that $(y^2 - 2xz - yz)^{p-1} \notin I$. This can be seen by noting that $(y^2 - 2xz - yz)^{p-1}$ contains the monomial y^{2p-2}, which does not appear in any degree $2p - 2$ form in $I\Bbbk[V]^C$. Now, we show that $(y^2 - 2xz - yz)^{(p-1)p} \in I^{[p]}$. From the a-invariant inequality, we see that

$$(y^2 - 2xz - yz)^p = y^{2p} - 2x^pz^p - y^pz^p \in I\,.$$

First note that in an expression of $y^{2p} - 2x^pz^p - y^pz^p$ as a combination of elements of I, $(y^p - z^{p-1}y)(N(x))$ cannot appear, since no other form of degree $2p$ has a nonzero x^pyz^{p-1} term. Thus, by degree considerations, we have

$$\begin{aligned} (y^2 - 2xz - yz)^p = &\sum_{a=0}^{\frac{p-1}{2}} (c_{1,a}(y^p - z^{p-1}y) + c_{2,a}N(x))z^{p-2a}(y^2 - 2xz - yz)^a \\ &+ \sum_{a=0}^{p-1} c_{3,a}z^{2p-2a}(y^2 - 2xz - yz)^a\,. \end{aligned}$$

Each exponent of z occuring is nonzero, and is strictly greater than one except when $a = \frac{p-1}{2}$ in the first sum. It follows that

$$(y^2-2xz-yz)^{p(p-1)} \equiv$$
$$(c_{1,\frac{p-1}{2}}(y^p - z^{p-1}y) + c_{2,\frac{p-1}{2}}N(x))^{p-1}z^{p-1}(y^2-2xz-yz)^{\frac{(p-1)^2}{2}} \pmod{z^p\Bbbk[V]^C}.$$

However, $\frac{(p-1)^2}{2} > p$ and the computation above shows that $(y^2-2xz-yz)^p \in z\Bbbk[V]^C$, so we conclude that $(y^2-2xz-yz)^{p(p-1)} \in z^p\Bbbk[V]^C \subset I^{[p]}$, as required.

Now, if $p \geqslant 3$, we show that $\Bbbk[V]^C$ is not F-regular. Notice that, in $\Bbbk[V]$, one has

$$\begin{aligned} N(x) &= \prod_{j=0}^{p-1}(x + jy + \binom{j}{2}z) \\ &\equiv \prod_{j=0}^{p-1}(x+jy) && \mod z\Bbbk[V] \\ &\equiv x^p - y^{p-1}x && \mod z\Bbbk[V] \end{aligned}$$

so that $(z, y^p - z^{p-1}y, N(x))\Bbbk[V] = (x^p, y^p, z)\Bbbk[V]$.

Now consider the element $(y^2-2xz-yz)^{(p+1)/2} \in \Bbbk[V]^C$.

$$\begin{aligned} (y^2-2xz-yz)^{(p+1)/2} &= (y^2 - z(2x+y))^{(p+1)/2} \\ &\equiv (y^2)^{(p+1)/2} && \mod (x^p, y^p, z)\Bbbk[V] \\ &\equiv y^{p+1} && \mod (x^p, y^p, z)\Bbbk[V] \\ &\equiv 0 && \mod (x^p, y^p, z)\Bbbk[V] \end{aligned}$$

and thus

$$(y^2-2xz-yz)^{(p+1)/2} \in (z, y^p - z^{p-1}y, N(x))\Bbbk[V].$$

We claim that

$$(y^2-2xz-yz)^{(p+1)/2} \notin (z, y^p - z^{p-1}y, N(x))\Bbbk[V]^C.$$

To see this, consider the grading on $\Bbbk[V]^C$. The element $(y^2-2xz-yz)^{(p+1)/2}$ has degree $p+1$, and degree considerations ensure that any element of $[(z, y^p - z^{p-1}y, N(x))\Bbbk[V]^C]_{p+1}$ is divisible by z, but $(y^2-2xz-yz)^{(p+1)/2}$ contains the monomial y^{p+1}, precluding this possibility. Since there is an element in $\Bbbk[V]^C$ and an ideal not containing it, but containment holds after expansion to $\Bbbk[V]$, we conclude that $\Bbbk[V]^C$ is not F-regular.

Theorem 2.11. *Put $C \cong \mathbb{Z}/p\mathbb{Z}$, and $\Bbbk$ a field of characteristic p. Let C be embedded as a subgroup of $\mathrm{GL}_n(\Bbbk)$ so that C acts linearly on $\Bbbk[V] = \Bbbk[x_1, \ldots, x_n]$. Assume that C contains no $\mathbf{V}_1$ summand.*

1. *The ring of invariants* $\Bbbk[V]^C$ *is Cohen-Macaulay if and only if* $C = \mathbf{V}_2$, $C = \mathbf{V}_2 \oplus \mathbf{V}_2$, *or* $p \geqslant 3$ *and* $C = \mathbf{V}_3$. *In each of these cases,* R^C *is a hypersurface.*

2. *The ring of invariants* $\Bbbk[V]^C$ *is strongly* F*-regular if and only if* $\Bbbk[V]^C$ *is* F*-rational if and only if* $C = \mathbf{V}_2$, *in which case* $\Bbbk[V]^C$ *is regular.*

3. *The ring of invariants* $\Bbbk[V]^C$ *is* F*-pure if* $C = \mathbf{V}_2$ *or* $C = \mathbf{V}_p^{\oplus a}$.

Proof. (1) We have checked that $\Bbbk[V]^C$ is a hypersurface or regular, in each of these cases. Conversely, any other representation of $\mathbb{Z}/p\mathbb{Z}$ is generated by an element that is not a bireflection.
(2) If $\Bbbk[V]^C$ is F-rational, then $\Bbbk[V]^C$ is Cohen-Macaulay, thus C is one of the representations listed in part (1). Note that if $p = 2$, then $\mathbf{V}_3$ is not a representation of $\mathbb{Z}/p$. We have thus verified the equivalence in each case.
(3) The only case in which we have not yet verifed this is for $C = \mathbf{V}_p$. After the change of coordinates

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{p-1} \\ x_p \end{bmatrix} \leftrightarrow \begin{bmatrix} x_1 \\ x_1 + x_2 \\ \vdots \\ x_1 + \binom{p-1}{1} x_2 + \cdots + \binom{p-1}{p-1} x_{p-1} \\ x_1 + \binom{p}{1} x_2 + \cdots + \binom{p}{p-1} x_{p-1} + \binom{p}{p} x_p \end{bmatrix}$$

the representation $\mathbf{V}_p$ is realized as the regular representation. Since this is a permutation representation, the ring of invariants is F-pure (see [23]). The same is true for $\mathbf{V}_p^{\oplus a}$. ∎

Question 2.12. In the context of the above theorem, is $\Bbbk[V]^C$ F-pure if and only if $C = \mathbf{V}_p^{\oplus b}$ or $C = \mathbf{V}_2 \oplus \mathbf{V}_p^{\oplus b}$ for some $b \in \mathbb{N}$? The following lemma helps limit the possibilities.

Lemma 2.13. *Let* G *be a finite subgroup of* $\mathrm{GL}_m(\Bbbk) \times \mathrm{GL}_n(\Bbbk)$. *One has compatible* G*-actions on* $\Bbbk[V] = \Bbbk[x_1, \ldots, x_m]$ *and* $\Bbbk[V \oplus W] = \Bbbk[x_1, \ldots, x_m, y_1, \ldots, y_n]$ *by restricting the action of* G *on* $V \oplus W$ *to* V. *The inclusion* $\Bbbk[V]^G \hookrightarrow \Bbbk[V \oplus W]^G$ *is split.*

Proof. The specialization map $\Bbbk[V \oplus W] \to R$ by setting the y variables to 0 is R-linear and fixes $\Bbbk$. This map takes $\Bbbk[V \oplus W]^G$ to $\Bbbk[V]^G$ and is $\Bbbk[V]^G$-linear and surjective. ∎

Proposition 2.14. (Chan [10]). *Let* G *be a finite subgroup of* $\mathrm{GL}(V)$, *with the induced linear action on* $\Bbbk[V] = \Bbbk[x_1, \ldots, x_n]$ *and* $\mathrm{char}(\Bbbk) = p$. *Let* P *be a* p*-Sylow subgroup of* G.

1. *If* $\Bbbk[V]^P$ *is strongly* F*-regular, then so is* $\Bbbk[V]^G$.

2. *If* $\Bbbk[V]^P$ *is* F*-pure, then so is* $\Bbbk[V]^G$.

Lemma 2.15. *In the context of the above proposition, if $\Bbbk[V]^P$ is Cohen-Macaulay, then so is $\Bbbk[V]^G$.*

Proof. The map $\mathrm{Tr}_P^G : \Bbbk[V]^P \to \Bbbk[V]^G$ given by

$$\mathrm{Tr}_P^G(r) = \sum_{\bar{g} \in G/P} \bar{g}(r)$$

is $\Bbbk[V]^G$-linear, and the following diagram commutes

$$\begin{array}{ccc} \Bbbk[V]^G & \xrightarrow{\quad 1 \quad} & \Bbbk[V]^G \\ & {\scriptstyle i} \searrow \quad \nearrow {\scriptstyle \frac{|P|}{|G|}\mathrm{Tr}_P^G} & \\ & \Bbbk[V]^P & \end{array} , \tag{2.2}$$

where i is the inclusion map. Note that $|G|/|P|$ is not divisible by p, and hence is a unit in $\Bbbk$. The rest of the proof proceeds exactly as in Theorem 1.9. ∎

Corollary 2.16. *Let G be a finite subgroup of $\mathrm{GL}(V)$, with the induced linear action on $\Bbbk[V] = \Bbbk[x_1, \ldots, x_n]$, with $\mathrm{char}(\Bbbk) = p$, and suppose that $|G| = ap$ with $\gcd(a, p) = 1$. Let $\sigma \in G$ have order p.*

1. *If $\langle \sigma \rangle$ gives the representation $\mathbf{V}_1^{\oplus n-2} \oplus \mathbf{V}_2$, then $\Bbbk[V]^G$ is F-regular.*
2. *If $\langle \sigma \rangle$ gives the representation $\mathbf{V}_1^{\oplus n-2} \oplus \mathbf{V}_2$ or $\mathbf{V}_1^{\oplus a} \oplus \mathbf{V}_p^{\oplus b}$ with $a + pb = n$, then $\Bbbk[V]^G$ is F-pure.*
3. *If $\langle \sigma \rangle$ gives the representation $\mathbf{V}_1^{\oplus n-2} \oplus \mathbf{V}_2$, $\mathbf{V}_1^{\oplus n-4} \oplus \mathbf{V}_2 \oplus \mathbf{V}_2$, or $\mathbf{V}_1^{\oplus n-3} \oplus \mathbf{V}_3$ with $p \geqslant 3$, then $\Bbbk[V]^G$ is Cohen-Macaulay.*

2.4 An application of the a-invariant

Lemma 2.17. *Let $\Bbbk$ be a field, and $\Bbbk[V] = \Bbbk[x_1, \ldots, x_n]$ be a polynomial ring. Let G be a finite subgroup of $\mathrm{GL}(V)$, and H a subgroup of G, acting naturally on $\Bbbk[V]$. Assume that $\Bbbk[V]^H$ and $\Bbbk[V]^G$ are Cohen-Macaulay. Then the inequality $a(\Bbbk[V]^G) \leqslant a(\Bbbk[V]^H)$ holds.*

Proof. Set $L = \mathrm{frac}(\Bbbk[V])$. We use the trace map

$$\mathrm{Tr}_H^G(r) = \sum_{\bar{g} \in G/H} \bar{g}(r) : \Bbbk[V]^H \to \Bbbk[V]^G .$$

The maps $\bar{g} : L^H \to L^H$, with $\bar{g} \in G/H$ are linearly independent over L^G. Since any element of L^H can be written as a fraction with a denominator in $\Bbbk[V]^G$, it follows that Tr_H^G is not the zero map.

Put

$$(-)^\vee = \underline{\mathrm{Hom}}_{\Bbbk[V]^G}(-, \omega_{\Bbbk[V]^G})\,.$$

Consider the sequence

$$\Bbbk[V]^H \xrightarrow{\mathrm{Tr}_H^G} \Bbbk[V]^G \longrightarrow \Bbbk[V]^G/\,\mathrm{Tr}_H^G(\Bbbk[V]^H) \longrightarrow 0\,.$$

Since $\mathrm{Tr}_H^G(\Bbbk[V])$ is not the zero ideal, $(\Bbbk[V]^G/\,\mathrm{Tr}_H^G(\Bbbk[V]))^\vee = 0$, so we have an embedding of graded $\Bbbk[V]^G$-modules

$$\begin{array}{ccccc} 0 & \longrightarrow & (\Bbbk[V]^G)^\vee & \xrightarrow{(\mathrm{Tr}_H^G)^\vee} & (\Bbbk[V]^H)^\vee \\ & & \sim\downarrow & & \sim\downarrow \\ 0 & \longrightarrow & \omega_{\Bbbk[V]^G} & \longrightarrow & \omega_{\Bbbk[V]^H}\,. \end{array} \tag{2.3}$$

where the vertical isomorphisms come from graded duality. Then the inequality

$$a(\Bbbk[V]^G) = \max\{t \mid [\omega_{\Bbbk[V]^G}]_{-t} \neq 0\} \leqslant \max\{t \mid [\omega_{\Bbbk[V]^H}]_{-t} \neq 0\} = a(\Bbbk[V]^H)$$

follows immediately. ∎

Theorem 2.18. *Let $\Bbbk$ be a field of characteristic $p > 0$, and $\Bbbk[V] = k[x_1, \ldots, x_n]$ be a polynomial ring. Let G be a finite subgroup of $\mathrm{GL}(V)$ where p divides $|G|$. If the inclusion $\Bbbk[V]^G \hookrightarrow \Bbbk[V]$ is $\Bbbk[V]^G$-split, then $a(\Bbbk[V]^G) < -n$.*

Proof. It follows from the hypothesis that $\Bbbk[V]^G \hookrightarrow \Bbbk[V]$ is $\Bbbk[V]^G$-split that $\Bbbk[V]^G$ is Cohen-Macaulay. Setting $H = 0$, Lemma 2.17 implies that $a(\Bbbk[V]^G) \leqslant -n$. Consider the n-th graded piece in (2.3). We have $a(\Bbbk[V]^G) = -n$ exactly when $[\omega_{\Bbbk[V]^G}]_n \neq 0$, and this holds if and only if $(\mathrm{Tr}^G)^\vee : [(\Bbbk[V]^G)^\vee]_n \longrightarrow [\Bbbk[V]^\vee]_n$ is a surjection of rank one $\Bbbk$-vector spaces. This is equivalent to each element

$$\phi \in [\Bbbk[V]^\vee]_n = [\underline{\mathrm{Hom}}_{\Bbbk[V]^G}(\Bbbk[V], \omega_{\Bbbk[V]^G})]_n = \mathrm{Hom}_{\Bbbk[V]^G}(\Bbbk[V], \omega_{\Bbbk[V]^G}(n))$$

factoring through the trace map, i.e., one has a commutative diagram of the form

$$\begin{array}{ccc} \Bbbk[V] & \xrightarrow{\phi} & \omega_{\Bbbk[V]^G}(n) \\ {\scriptstyle \mathrm{Tr}^G}\downarrow & \nearrow & \\ \Bbbk[V]^G\,. & & \end{array}$$

Then, since $\mathrm{Tr}^G(1) = |G| = 0$, we have $\phi(1) = 0$.

Let $0 \neq w \in [\omega_{\Bbbk[V]^G}]_n$. Then there is a surjective $\Bbbk[V]^G$-linear map ρ and an $\Bbbk[V]^G$-linear map $\times w : \Bbbk[V]^G \to \omega_{\Bbbk[V]^G}(n)$ taking $1 \mapsto w$. The composition

$$(\times w \circ \rho) : \Bbbk[V] \to \omega_{\Bbbk[V]^G}(n)$$

is a degree-preserving $\Bbbk[V]^G$-linear map with $(\times w \circ \rho)(1) = w$, contradicting that 1 is in the kernel of such a map. ∎

Remark 2.19. The same proof shows moreover that if G acts by degree-preserving automorphisms on a Gorenstein ring R, $\mathrm{char}(\Bbbk)$ divides $|G|$, and $a(R^G) = a(R)$, then the inclusion map is not split.

Remark 2.20. In the proof above, by applying local duality, one can rephrase the key obstruction in terms of local cohomology. Specifically, if $a(\Bbbk[V]^G) = a(\Bbbk[V])$ and the action of G is modular, then $\mathrm{H}^d_{\mathfrak{m}_{\Bbbk[V]}}(\Bbbk[V])$ does not surject onto $\mathrm{H}^d_{\mathfrak{m}_{\Bbbk[V]^G}}(\Bbbk[V]^G)$.

Corollary 2.21. *Let $\Bbbk$ be a field of characteristic $p > 0$, and $\Bbbk[V] = k[x_1, \ldots, x_n]$ be a polynomial ring. Let G be a finite subgroup of the symmetric group $\mathcal{S}_n$ with p dividing $|G|$, acting on $\Bbbk[V]$ by permuting variables. If G is contained in $\mathcal{A}_n$, then $\Bbbk[V]^G \hookrightarrow \Bbbk[V]$ is not $\Bbbk[V]^G$-split.*

Proof. In any characteristic, $\Bbbk[V]^{\mathcal{A}_n} = k[e_1, \ldots, e_n, \Delta]$, where e_i is the i-th symmetric polynomial, and

$$\Delta = \sum_{\sigma \in \mathcal{A}_n} (x^0_{\sigma(1)} x^1_{\sigma(2)} \cdots x^{n-2}_{\sigma(n-1)} x^{n-1}_{\sigma(n)}) .$$

In this hypersurface, $\Delta^2 \in (e_1, \ldots, e_n)$, so Δ generates the socle modulo the system of parameters $(e_1, \ldots, e_n)$. Thus

$$a(\Bbbk[V]^{\mathcal{A}_n}) = \deg(\Delta) - \deg(e_1) - \cdots - \deg(e_n) = -n$$

If $\Bbbk[V]^G$ is not Cohen-Macaulay, we are done. Otherwise, by Lemma 2.17, applied to G as a subgroup of $\mathcal{A}_n$, $a(\Bbbk[V]^G) = -n$. By Theorem 2.18, $\Bbbk[V]^G \hookrightarrow R$ is not $\Bbbk[V]^G$-split. ∎

Conjecture 2.22. (Broer [7]). Let P in $\mathrm{GL}_n(\Bbbk)$ be a p-group. If $\Bbbk[V]^P$ is F-regular, must $\Bbbk[V]^P$ in fact be a polynomial ring?

We note that the conjecture holds for an example considered in the introduction.

Example 2.23. Let G be the group from Example 1.8. Note that G is a p-group, and recall that G has the property that each stabilizer subspace is generated by pseudoreflections. We have

$$\Bbbk[V]^G \cong \frac{\Bbbk\big[x_1, x_2, w, z_1, z_2\big]}{\Big(w^p - x_1^p z_1 - x_2^p z_2 - w\big(\sum_{j=1}^{p}(x_1^{p-j+1}x_2^j)^{p-1}\big)\Big)}.$$

Note that $w^p \in (x_1, x_2)^{[p]} \subseteq (x_1, x_2, z_1, z_2)^{[p]}$. In particular, (x_1, x_2) is a parameter ideal. Since $w \notin (x_1, x_2)$, the ring of invariants is not F-regular.

CHAPTER 3

F-SIGNATURE OF TORIC RINGS

3.1 Introduction

In this section, we consider the F-signature of another class of invariant rings. The n-dimensional torus $(\Bbbk^*)^n$ is the direct product of n copies of the multiplicative group of the field $\Bbbk$. Tori are linearly reductive in all characteristics, so rings of invariants of tori acting on $\Bbbk[V]$ are direct summands of the polynomial ring, and hence, if the characteristic of $\Bbbk$ is positive, strongly F-regular.

A ring of invariants of a torus action may be written in the form $R = \Bbbk[M \cap \sigma]$ where $M \cong \mathbb{Z}^d$ is a lattice and $\sigma \subset M \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^d$ is a cone: a subsemigroup of $\mathbb{R}^d$ that is a convex set. Singh [38], Watanabe–Yoshida [45], and Von Korff [43] have studied the F-signature of toric rings before, and a formula for the F-signature in terms of the cone exists. However, the structure of the set of values of the F-signature among all toric varieties has not yet been thoroughly studied. We do this below, with the goal of shedding more light on the behavior of this invariant and what information it contains about singularities.

3.2 Bounds on F-signature

Definition 3.1. Let $L \cong \mathbb{Z}^d$ be a lattice. For $v_1, \ldots, v_n \in L^\vee$, a set of vectors in the dual lattice, define the polytope

$$\mathcal{P}^\vee(\{v_1, \ldots, v_n\}) = \{w \in L \otimes_{\mathbb{Z}} \mathbb{R} \mid w \cdot v_i \in [0,1]\}\,.$$

Definition 3.2. Let R be a normal affine toric variety without torus factors. Write $R = \Bbbk[M \cap \sigma]$ where $M \cong \mathbb{Z}^d$ is a lattice and $\sigma \subset M \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^d$ is a cone. Let $v_1, \ldots, v_n \in M^\vee$ be primitive generators for $\sigma^\vee$. The *Watanabe-Yoshida polytope* of R is defined to be $\mathcal{WY}(R) = \mathcal{P}^\vee(\{v_1, \ldots, v_n\})$.

Theorem 3.3. (Von Korff, Watanabe–Yoshida [43, 45]). *In the context of the previous definition, the F-signature of R is the volume of $\mathcal{WY}(R)$.*

Proposition 3.4. *The volume of the portion of the unit d-cube where the sum of the coordinates lies between k and $k+1$ is $\dfrac{A(d,k)}{d!}$, where $A(d,k)$ denotes the Eulerian number with parameters d and k.*

Proof. The following argument is due to Stanley [41]. The hyperplanes $x_i = x_j$ cut the interior of the unit cube into $d!$ simplices of equal volume. Each can be characterized as the set of points Δ_σ where $0 < x_{\sigma(1)} < x_{\sigma(2)} < \cdots < x_{\sigma(d)} < 1$ for some $\sigma \in \mathcal{S}_d$, giving a natural bijection between the simplices and $\mathcal{S}_d$. Define a map

$$\phi(x_1,\ldots,x_d)_i = \begin{cases} x_{i+1} - x_i & \text{if } x_i < x_{i+1} \text{ and } i \neq d \\ 1 + x_{i+1} - x_i & \text{if } x_i > x_{i+1} \text{ and } i \neq d \\ 1 - x_n & \text{if } i = d\,. \end{cases}$$

Note that ϕ maps into the unit cube, and that $\phi|_{\Delta_\sigma}$ is affine with determinant ± 1. Further, if $(x_1,\ldots,x_d) \in \Delta_\sigma$, then

$$k \leqslant \phi(x_1,\ldots,x_d)_1 + \cdots + \phi(x_1,\ldots,x_d)_d \leqslant k+1\,,$$

where k is the number of descents of σ. Additionally, the map

$$\psi(x_1,\ldots,x_d)_i = \lceil x_i + \cdots + x_n \rceil - (x_i + \cdots + x_n)$$

provides an inverse for ϕ on its image. ∎

Lemma 3.5. *For the Eulerian numbers $A(d,k)$, the following hold:*

(a) $\dfrac{A(d,k)}{d!} > 1/2$ *if and only if* $(d,k) = (1,0)$, $(3,1)$, *or* $(5,2)$.

(b) $\lim\limits_{d\to\infty} \max\limits_{k<d} \dfrac{A(d,k)}{d!} = 0\,.$

Proof. (a) By symmetry, it is clear that $\dfrac{A(d,k)}{d!} < 1/2$ for an even integer d. Let $k \geqslant 3$; we will show that $\dfrac{A(2k+1,k+j)}{(2k+1)!} < 1/2$ by induction. The values can explicitly checked for $k = 3$. By twice applying the relation

$$A(n,m) = (n-m)\ A(n-1,m-1) + (m+1)\ A(n-1,m)$$

one obtains the equality

$$\begin{aligned} A(2k+1,k+j) =& (k-j+1)!\ A(2k-1,k-j-2) + (k+j+1)!\ A(2k-1,k-j) \\ &+ 2(k^2+k-j^2)\ A(2k-1,k-j-1)\,. \end{aligned}$$

By induction, this is less than $(2k-1)!\ (k^2 + (3/2)k + 1/2)$, which, for $k \geqslant 3$, is less $(1/2)(2k+1)!$ as required.

(b) The volume of the portion of the unit d-cube where the sum of the coordinates lies between k and $k+1$ can be interpreted as the probability that the sum of d independent uniform random variables $X_1, \ldots, X_d$ is between k and $k+1$. Now,

$$\mathbb{P}\left[k \leqslant \sum_{i=1}^{d} X_i \leqslant k+1\right] = \mathbb{P}\left[\sqrt{d}\left(\frac{k}{d} - \frac{1}{2}\right) \leqslant \sqrt{d}\left(\frac{\sum X_i}{d} - \frac{1}{2}\right) \leqslant \sqrt{d}\left(\frac{k+1}{d} - \frac{1}{2}\right)\right].$$

This probability tends to 0 uniformly in k as $d \to \infty$, since the random variable

$$\sqrt{d}\left(\frac{\sum X_i}{d} - \frac{1}{2}\right)$$

converges to the normal distribution $N(0, 1/12)$ by the central limit theorem. ∎

Theorem 3.6. *The largest F-signature of a singular affine toric variety is $2/3$, achieved in dimension 3. The second largest such value is $11/20$, achieved in dimension 5. No other value greater than $1/2$ is achieved.*

Proof. We may assume that the affine toric variety has no torus factors. Write $R = \Bbbk[M \cap \sigma]$ where $M \cong \mathbb{Z}^d$ is a lattice and $\sigma \subset M \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^d$ is a cone. Let $v_1, \ldots, v_n \in M^\vee$ be primitive generators for $\sigma^\vee$.

$$\mathcal{WY}(R) = \bigcap_{\substack{J \subset \{1,\ldots,n\} \\ |J|=d}} \mathcal{P}^\vee(\{v_{j_1}, \ldots, v_{j_d}\}). \tag{3.1}$$

By the Jacobian formula,

$$\operatorname{vol}(\mathcal{P}^\vee(\{v_{j_1}, \ldots, v_{j_d}\})) = \left|\frac{1}{\det[v_{j_1}, \ldots, v_{j_d}]}\right|.$$

Thus, if $s(R) > 1/2$, $|\det[v_{j_1}, \ldots, v_{j_d}]| = 1$ for any $J \subset \{1, \ldots, n\}$ with $|J| = d$. Assume for now that this is the case. If $n = d$, then $\{v_1, \ldots, v_n\}$ is a basis for $M^\vee$, so R is nonsingular. If $n > d$, and $\sigma'^\vee = \{v_1, \ldots, v_{d+1}\}$, then $s(\Bbbk[L \cap \sigma]) \leqslant s(\Bbbk[L \cap \sigma'])$. Consider the case where $n = d+1$. The vectors $\{v_1, \ldots, v_d\}$ form a basis for $L^\vee$; we compute the volume of $\mathcal{WY}(R)$ in these coordinates. Since $|\det[v_1, \ldots, \widehat{v_i}, \ldots, v_d, v_{d+1}]| = 1$, the i^{th} coordinate of v_{d+1} is ± 1. That is, in suitable coordinates,

$$[v_1, \ldots, v_{d+1}] = \begin{bmatrix} 1 & 0 & \ldots & 0 & \pm 1 \\ 0 & 1 & \ldots & 0 & \pm 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & \pm 1 \end{bmatrix}.$$

Note that if $d \leqslant 2$, we get a redundant cone generator for $\sigma^\vee$, so we may assume that $d \geqslant 3$. Put $x_1, \ldots, x_d$ for coordinates of L forming a dual basis to $v_1, \ldots, v_d$. Renumber

the coordinates so that in the matrix above, $x_i \cdot v_{d+1} = +1$ for $i \leqslant k$ and $x_i \cdot v_{d+1} = -1$ for $i > k$. Then $\mathcal{P}^\vee(\{v_1, \ldots, v_{d+1}\})$ is the subset of the unit d-cube where

$$0 \leqslant x_1 + \cdots + x_k - x_{k+1} - \cdots - x_d \leqslant 1\,.$$

Using $x_j \mapsto 1 - x_j$ symmetry of the cube, we have

$$\mathrm{vol}(\mathcal{P}^\vee(\{v_1, \ldots, v_{d+1}\})) = \mathrm{vol}(\{(x_1, \ldots, x_d) \in [0,1]^d \mid k \leqslant \sum_{i=1}^{d} x_i \leqslant k+1\})\,.$$

By the Lemma 3.5, we see that the volume s is greater than $1/2$ only if $d = 3$ and $k = 1$ or $d = 5$ and $k = 2$. We now consider what happens if $n \geqslant d+2$. If $\mathrm{vol}(\mathcal{P}^\vee(\{v_1, \ldots, v_n\})) > 1/2$, with $d = 3$, then

$$[v_1, \ldots, v_4] = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

in the dual basis to v_1, v_2, v_3. If $n \geqslant 5$, the same arguments show that if $s > 1/2$, in a particular basis we have

$$[v_1, \ldots, v_5] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 & 1 \end{bmatrix}$$

where one computes $\mathrm{vol}(\mathcal{P}^\vee(\{v_1, \ldots, v_5\})) = 1/3$. Thus, the F-signature cannot be greater than $1/2$ in this case. Now consider when $d = 5$. If $\mathrm{vol}(\mathcal{P}^\vee(\{v_1, \ldots, v_n\})) > 1/2$,

$$[v_1, \ldots, v_6] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

in the dual basis to v_1, v_2, v_3, v_4, v_5. If $n \geqslant 7$, a case-by-case analysis similar to above shows that $s < 1/2$.

If $s(R) = 1/2$, then $|\det[v_{j_1}, \ldots, v_{j_d}]| \leqslant 2$ for all $J \subset \{1, \ldots, n\}$ with $|J| = d$. The case where $|\det[v_{j_1}, \ldots, v_{j_d}]| = 1$ for all $J \subset \{1, \ldots, n\}$ with $|J| = d$ was discussed above, and no toric ring with F-signature equal to $1/2$ occurs in this case. Thus, assume that $|\det[v_1, \ldots, v_d]| = 2$. One may choose a basis for L such that

$$[v_1, \ldots, v_d] = \begin{bmatrix} 2 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}$$

If $n > d$, then the F-signature is strictly less than $\mathrm{vol}(\mathcal{P}^\vee(\{v_1, \ldots, v_d\})) = 1/2$. ∎

Example 3.7. The affine toric variety with dual cone generators

$$[v_1, \ldots, v_{d+1}] = \begin{bmatrix} 1 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -1 \end{bmatrix}$$

where the last column has k positive entries and $d-k$ negative entries is isomorphic to the affine cone over $\mathbb{P}^{k-1} \times \mathbb{P}^{d-k}$. Singh showed that the F-signature of this ring is $\frac{A(d,k)}{d!}$. The proof above, combined with Stanley's result, gives a combinatorial interpretation of this calculation.

CHAPTER 4

SEPARATING SETS AND LOCAL COHOMOLOGY

The results and exposition of this chapter represent the joint work of Emilie Dufresne and myself, and appear in the published paper [18][1].

4.1 Introduction

For an action of an algebraic group on a vector space V, a *separating set* is a collection of invariants that, as functions on V in $\Bbbk[V]$, distinguish any two points that can be distinguished by some invariant. While using invariants as a tool to distinguish orbits of a group action on a variety is a classical endeavor, this approach to invariant theory has enjoyed a resurgence of interest in its modern form, initiated by the work of Derksen and Kemper [13, 29].

We will assume throughout this section that $\Bbbk$ is algebraically closed, G is finite, and V has dimension d. While the results below have analogous statements over general fields (see Remark 4.4), the exposition is cleaner with the assumption that $\Bbbk$ is algebraically closed. In this setting, a separating set is a subset $E \subset \Bbbk[V]^G$ such that, if, for $v, w \in V$, the orbits $G \cdot v$ and $G \cdot w$ are distinct, then there is an $h \in E$ with $h(v) \neq h(w)$; that is, a separating set is a set of invariants that separates orbits.

While the ring of invariants (or a generating set for it) forms a separating set, there often exist smaller and/or otherwise better-behaved separating sets — especially in the *modular* case, where $|G|$ is not invertible in $\Bbbk$. For example, there always exist separating sets consisting of elements of degree at most $|G|$ ([13, Corollary 3.9.14]), and polarizations of separating sets yield separating sets for vector invariants ([14, Theorem 1.4]). The main question we consider in this paper is: What is the least cardinality of a separating set?

---

[1]Reprinted with permission of Elsevier:
E. Dufresne and J. Jeffries, Separating invariants and local cohomology, Adv. Math., 270 (2015), pp. 565–581.
http://www.sciencedirect.com/science/article/pii/S0001870814003788

Some general bounds are known. It follows from [13, Proposition 2.3.10] that the algebra generated by a separating set, i.e., a *separating algebra*, has dimension d; thus any separating set has at least d elements. On the other hand, a secant variety argument (see [15, Proposition 5.1.1]) shows that there always exists a separating set of size $2d+1$.

Since any separating algebra has dimension d, the existence of a separating set of size d is equivalent to the existence of a polynomial separating algebra. In [16, Theorem 1.1], Dufresne extends Serre's result by showing that if there exists a polynomial separating algebra, then G is a reflection group. As a corollary, in the nonmodular case, there exists a polynomial separating algebra if and only if G is a reflection group. The existence of a separating set of size d is thus related to whether G is a reflection group. Further, in [16, Theorem 1.3], Dufresne shows that if there is a graded separating algebra that is a complete intersection, then the action of G is generated by *bireflections* — elements that fix a codimension two subspace in V. Consequently, if there is a separating set consisting of $d+1$ homogeneous invariants (whence the algebra it generates is a graded hypersurface and hence a complete intersection), then the action of G is generated by bireflections.

Below, we apply techniques of local cohomology to strengthen and extend these bounds. After reviewing some preliminary notions in Section 4.2, in Section 4.3, we obtain our main result.

Theorem 4.1. *If there exists a separating set of size $d+r-1$, then every isotropy subgroup G_U is generated by r-reflections. In particular, G is generated by r-reflections.*

Setting $r=1$, we obtain the following strengthening of [16, Theorem 1.1]: If there exists a separating set of size d, then G is a rigid reflection group. Our approach utilizes Àlvarez Montaner, García López, and Zarzuela Armengou's computation of local cohomology with support in a subspace arrangement in [2]. Their formula is a local cohomology analogue of the Goresky-MacPherson formula for the singular cohomology of the complement of a real subspace arrangement (see, e.g., [44, Theorem 1.3.8]); in this way, one can consider our results a link between the Goresky-MacPherson formula and the Shephard-Todd theorem.

In Section 4.4, we focus on rigid reflection groups. Applying techniques from poset homology, we show that the cohomological obstructions to small separating sets in Section 4.3 vanish for all integers greater than d. While there are rigid reflection groups for which the ring of invariants is not polynomial, some of the counterexamples have been proved to have a polynomial separating algebra, e.g., [16, Example 3.1]. We pose the conjecture that there exists a polynomial separating algebra if and only if G is a rigid reflection group.

In Section 4.5, we construct a variety of examples of separating sets for which the lower bound from the main theorem is realized: that is, we construct separating sets of the minimal possible cardinality. While we do not have a specific algorithm by which we create such sets, we are able to use an idea from Dufresne's thesis [15, Section 5.2] (the "triangle trick") effectively in a wide range of cases.

4.2 Preliminaries

For any subset U of V, we define its *isotropy subgroup* G_U as follows:

$$G_U := \{\sigma \in G \mid \sigma \cdot u = u,\ \forall u \in U\}\,.$$

An element $\sigma \in G$ is called an *r-reflection* if its fixed subspace V^σ has codimension at most r. In particular, a 1-reflection is a pseudoreflection, and a 2-reflection is a bireflection. We say that G is an *r-reflection group* if it is generated by elements whose fixed space has codimension at most r.

A linear subspace $W \subset V$ is an *r-reflecting subspace* if and only if W has codimension r in V and its isotropy subgroup G_W is nontrivial. An r-reflecting subspace will be called *minimal* if it is not the intersection of r'-reflecting subspaces with $r' < r$. A group is called a *rigid r-reflection group* if every minimal reflecting subspace has codimension at most r. This is equivalent to requiring that every isotropy subgroup is an r-reflection group. We will say that G is a *(rigid) $(<r)$-reflection group* if there exists an $r' < r$ such that G is a (rigid) r'-reflection group. For $r = 1$ we will say *(rigid) reflection group* instead of (rigid) 1-reflection group.

In the nonmodular case, it follows from the Shephard-Todd theorem and Serre's theorem that every reflection group is a rigid reflection group. For $r > 1$, the condition of being a rigid r-reflection group is stronger than that of being an r-reflection group. For example, let V be a $(2n+1)$-dimensional vector space over $\mathbb{C}$ with basis $u_1, \ldots, u_n, v_1, \ldots, v_n, w$ and let $G := C_2 \times C_2 = \langle \alpha, \beta \rangle$ act on V by

$$\begin{aligned}
&\alpha(u_i) = -u_i \qquad && \beta(u_i) = u_i && \text{for } i = 1, \ldots, n\,,\\
&\alpha(v_i) = v_i && \beta(v_i) = -v_i && \text{for } i = 1, \ldots, n\,,\\
&\alpha(w) = -w && \beta(w) = -w\,. &&
\end{aligned}$$

Here G is generated by $(n+1)$-reflections, but $\langle \alpha\beta \rangle$ is an isotropy subgroup of G generated by a $(2n)$-reflection, thus G is not a rigid $(<2n)$-reflection group.

The *separating variety* $\mathcal{S}_{V,G}$ is a closed subvariety of the product $V \times V$ that completely determines the equivalence relation induced by $\Bbbk[V]^G$ on V. More precisely, we have

$$\mathcal{S}_{V,G} := \{(u,v) \in V \times V \mid f(u) = f(v), \text{ for all } f \in \Bbbk[V]^G\} \tag{4.1}$$

$$= \mathcal{V}_{V\times V}(f \otimes 1 - 1 \otimes f \mid f \in \Bbbk[V]^G)\,. \tag{4.2}$$

A separating set can then be characterized as a subset $E \subset \Bbbk[V]^G$ that cuts out the separating variety in $V \times V$, that is, such that $\mathcal{V}_{V\times V}(f \otimes 1 - 1 \otimes f \mid f \in E) = \mathcal{S}_{V,G}$. In ideal-theoretic terms, let

$$\mathcal{I}(\mathcal{S}_{V,G}) := \sqrt{(h \otimes 1 - 1 \otimes h \mid h \in \Bbbk[V]^G)} \subset \Bbbk[V^2] := \Bbbk[V \times V]\,.$$

Proposition 4.2. ([29]). *A set of invariants $\{f_1, \ldots, f_t\}$ is a separating set for G acting on V if and only if*

$$\sqrt{(f_1 \otimes 1 - 1 \otimes f_1, \ldots, f_t \otimes 1 - 1 \otimes f_t)} = \mathcal{I}(\mathcal{S}_{V,G})\,.$$

For actions of finite groups, the invariants actually separate orbits (see, for example, [14, Lemma 2.1]) and so the separating variety coincides with the graph of the action

$$\Gamma_{V,G} := \{(v, \sigma \cdot v) \mid v \in V,\ \sigma \in G\}\,.$$

This provides significant geometric insight into $\mathcal{S}_{V,G}$:

Lemma 4.3. ([16]). *Let G be a finite group acting linearly on V.*

(a) The separating variety has an irreducible decomposition of the form

$$\mathcal{S}_{V,G} = \bigcup_{\sigma \in G} (1 \otimes \sigma)(V)$$

with each $(1 \otimes \sigma)(V)$ a linear subspace isomorphic to V.

(b) If $\sigma, \tau \in G$, then $(1 \otimes \sigma)(V) \cap (1 \otimes \tau)(V) = (1 \otimes \tau)(V^{\tau^{-1}\sigma})$, which has dimension equal to that of the subspace fixed by $\tau^{-1}\sigma$ in V. Every nonempty intersection of components $(1 \otimes \sigma)(V)$ with $\sigma \in G$ is of the form $(1 \otimes \gamma)(V^H)$, where $H \leq G$ is an isotropy subgroup, and $\gamma \in G/H$.

Remark 4.4. The assumption that $\Bbbk$ is algebraically closed is essential in Proposition 4.2. However, one may obtain results in the nonalgebraically closed case by considering a *geometric separating set*: for G finite, this is a subset of $\Bbbk[V]^G$ that separates orbits of G in $V \otimes_{\Bbbk} \bar{\Bbbk}$ (see [16, Section 2]). By [16, Theorem 2.1], a geometric separating set is

characterized by the ideal-theoretic equality in Proposition 4.2. Accordingly, the results of Section 4.3 hold for $\Bbbk \neq \bar{\Bbbk}$ if one replaces the phrase "separating set" with "geometric separating set." Further, since $\Bbbk[V]^G$ is a geometric separating set, Corollary 4.10 holds verbatim for all $\Bbbk$.

For an arrangement of linear subspaces $X \subset \mathbb{A}^m$, let $P(X)$ denote the *intersection poset* of X: the collection, ordered by inclusion, of linear subspaces that occur as intersections of components of X. For $p \in P(X)$, the *interval* $P(>p)$ is the subposet of $P(X)$ consisting of elements containing p. One defines $P(<p), P(\geqslant p)$, and $P(\leqslant p)$ analogously. The reduced homology of a poset P with coefficients in $\Bbbk$ will be denoted by $\widetilde{\mathrm{H}}_\bullet(P;\Bbbk)$; this is the reduced simplicial homology of the simplicial complex whose vertices are elements of the poset, and whose faces are the chains.

In our setting, for a linear action of a finite group, the separating variety $\mathcal{S}_{V,G}$ is a subspace arrangement. By abuse of notation, we will also denote its intersection poset by $\mathcal{S}_{V,G}$. Note that if $W \subseteq V$ is a subspace, then $\mathcal{S}_{V,G}(>(1\otimes 1)(W)) \cong \mathcal{S}_{V,G_W}(>(1\otimes 1)(W))$.

We will also consider the poset $\mathcal{R}_{V,G}$ of r-reflecting subspaces (all possible r's). The two posets $\mathcal{S}_{V,G}$ and $\mathcal{R}_{V,G}$ are related by the following lemma.

Lemma 4.5. *For any $\sigma \in G$, the interval $\mathcal{S}_{V,G}(<(1\otimes\sigma)(V))$ is isomorphic to $\mathcal{R}_{V,G}$.*

Proof. The map on $\Gamma_{V,G}$ given by applying σ to the second coordinate is an isomorphism, thus $\mathcal{S}_{V,G}(\leqslant(1\otimes\sigma)(V)) \cong \mathcal{S}_{V,G}(\leqslant(1\otimes 1)(V))$. Now,

$$\begin{aligned}(1\otimes 1)(V)\cap(1\otimes\sigma_1)(V)\cap\cdots\cap(1\otimes\sigma_m)(V)&\\ &= \{(v,v)\,|\,v=\sigma_1(v)=\cdots=\sigma_m(v)\}\\ &= (1\otimes 1)(V^{\langle\sigma_1,\ldots,\sigma_m\rangle})\,,\end{aligned}$$

so that the intersections of components of $\mathcal{S}_{V,G}$ contained in $(1\otimes 1)(V)$ coincide with the diagonal embeddings of reflecting subspaces. ∎

It is worth noting that the order on $\mathcal{R}_{V,G}$ used here is dual to that most commonly used in the literature on subspace arrangements.

4.3 Lower bounds on the size of separating sets

In this section, we give a lower bound on the size of a separating set for a ring of invariants of a finite group. We reiterate the assumption that $\Bbbk$ is algebraically closed; see Remark 4.4 for the nonalgebraically closed case. The following lemma will be key to our applications.

Lemma 4.6. *The separating variety is connected in codimension $\leqslant r$ if and only if the action of G is generated by $(\leqslant r)$-reflections.*

Proof. By Lemma 4.3 (a), the separating variety $\mathcal{S}_{V,G}$ is connected in codimension $\leqslant r$ if and only if, for any $\sigma, \sigma' \in G$, there is a sequence of components

$$(1 \otimes \sigma)(V) = (1 \otimes \sigma_0)(V) \ , \ (1 \otimes \sigma_1)(V) \ , \ \dots \ , \ (1 \otimes \sigma_r)(V) = (1 \otimes \sigma')(V)$$

such that $(1 \otimes \sigma_i)(V) \cap (1 \otimes \sigma_{i+1})(V)$ has codimension $\leqslant r$. By Lemma 4.3 (b),

$$\dim (1 \otimes \sigma_i)(V) \cap (1 \otimes \sigma_{i+1})(V) = \dim V^{\sigma_{i+1}^{-1}\sigma_i} .$$

Thus, $\mathcal{S}_{V,G}$ is connected in codimension $\leqslant r$ if and only if for any $\sigma, \sigma' \in G$ there exist $(\leqslant r)$-reflections

$$\tau_1 = \sigma_0^{-1}\sigma_1 \ , \ \tau_2 = \sigma_1^{-1}\sigma_2 \ , \ \dots \ , \ \tau_r = \sigma_{r-1}^{-1}\sigma_r$$

such that $\sigma = \tau_1 \cdots \tau_r \sigma'$. However, this just means that G is generated by $(\leqslant r)$-reflections. ∎

We first note that a connectedness theorem of Grothendieck allows for the following generalization of [16, Theorem 1.1].

Proposition 4.7. *If there exists a separating set of size $d + r - 1$, then the action of G is generated by $(\leqslant r)$-reflections.*

Proof. By Proposition 4.2, if there is a separating set of size $d + r - 1$, then $\mathcal{I}(\mathcal{S}_{V,G})$ is set-theoretically defined by $d + r - 1$ equations. By [20, Exposé XIII, Théorème 2.1], if $\mathcal{I}(\mathcal{S}_{V,G})$ can be set-theoretically cut out by $d + r - 1$ or fewer equations, then $\mathcal{S}_{V,G}$ is connected in codimension $\leqslant r$. Then, by Lemma 4.6, G is generated by $(\leqslant r)$-reflections. ∎

A stronger result can be obtained by examining the local cohomology with support in $\mathcal{I}(\mathcal{S}_{V,G})$. Local cohomology with support in a subspace arrangement is studied by Àlvarez Montaner, García López, and Zarzuela Armengou in [2]. Following along the lines of Björner and Ekedahl's computation of ℓ-adic cohomology of such spaces, they establish a Mayer-Vietoris spectral sequence for local cohomology and show that it degenerates for subspace arrangements, thus obtaining a Goresky-MacPherson analogue in local cohomology. In particular, their formula provides a combinatorial characterization of the vanishing and nonvanishing of the local cohomology modules.

Theorem 4.8. *(a)* ([2, p. 39], [30, Theorem 2.1]). *If $I_1, \dots, I_t \subset R$ are ideals, and M an R-module, then there is a Mayer-Vietoris spectral sequence*

$$E_1^{-p,q} = \bigoplus_{i_0<\cdots<i_p} \mathrm{H}^q_{I_{i_0}+\cdots+I_{i_p}}(M) \quad \Longrightarrow \quad \mathrm{H}^{q-p}_{I_1\cap\cdots\cap I_t}(M)\,.$$

(b) ([2, Corollary 1.3]). *If $I_1, \dots, I_t \subset R$ are ideals of linear subspaces in a polynomial ring, then the spectral sequence above degenerates at E_2, and for all $q \geqslant 0$ there is an associated graded module of the local cohomology module $\mathrm{H}^q_{I_1\cap\cdots\cap I_t}(R)$ with*

$$\operatorname{gr}\left(\mathrm{H}^q_{I_1\cap\cdots\cap I_t}(R)\right) \cong \bigoplus_{p\in P} \left[\mathrm{H}^{\operatorname{codim}(p)}_{I(p)}(R) \otimes_{\Bbbk} \widetilde{\mathrm{H}}_{\operatorname{codim}(p)-q-1}(P(>p);\Bbbk)\right],$$

where P is the intersection poset of $\mathcal{V}(I_1 \cap \cdots \cap I_t)$.

With this description of the local cohomology, we obtain the following strengthening of Proposition 4.7.

Theorem 4.9. *Let $r_1, \dots, r_s$ be the codimensions of minimal reflecting subspaces. Then $\mathrm{H}^{d+r_i-1}_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) \neq 0$. In particular, if r is the maximal codimension of a minimal reflecting subspace, then every separating set has size at least $d+r-1$.*

Proof. Let $W \subset V$ be a minimal r-reflecting subspace in the sense of Subsection 4.2. Note that

$$\mathcal{S}_{V,G}(>(1\otimes 1)(W)) \cong \mathcal{S}_{V,G_W}(>(1\otimes 1)(V^{G_W}))\,.$$

The latter poset is connected if and only if $\mathcal{S}_{V,G_W}$ is connected in codimension $< r$. By Lemma 4.6, this is the case if and only if G_W is generated by $(<r)$-reflections. Since W is minimal, G_W is not generated by $(<r)$-reflections: if $G_W = \langle g_1, \dots, g_s\rangle$ with each g_i an $(<r)$-reflection, one may write $W = \bigcap_{i=1}^s V^{\langle g_i\rangle}$, expressing W as the intersection of larger reflecting subspaces. Thus,

$$\widetilde{\mathrm{H}}_0\left(\mathcal{S}_{V,G}(>(1\otimes 1)(W));\Bbbk\right) \neq 0\,.$$

Theorem 4.8 (b) applies to show that $\mathrm{H}^{d+r-1}_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) \neq 0$. Thus, $\mathcal{I}(\mathcal{S}_{V,G})$ cannot be set-theoretically defined by $d+r-1$ or fewer equations, and by Proposition 4.2, any separating set has size at least $d+r-1$. ∎

Corollary 4.10. *If r is the maximal codimension of a minimal reflecting subspace, then the embedding dimension of $\Bbbk[V]^G$ is at least $d+r-1$.*

Proof. This follows immediately from Theorem 4.9 since a minimal generating set is a separating set. Alternatively, one may argue by using Proposition 4.7 to conclude that the embedding codimension is at least r if G is not a $(<r)$-reflection group, and applying [28, Theorem A], according to which the embedding codimension (referred to in *ibid.* as the polynomial defect) does not increase when passing to the invariants of an isotropy subgroup. ∎

Remark 4.11. In the recent work of Reimers [33, Theorem 2.4], the statement of Lemma 4.6 is established in the more general setting where G acts on a variety that is connected in codimension $\leqslant r$. This result is then applied to study the depth of schemes defining the separating variety of the action — particularly, in terms of local cohomology, the least i for which $\mathrm{H}^i_{\mathfrak{m}}(R/J) \neq 0$ for some J with $\sqrt{J} = \mathcal{I}(\mathcal{S}_{V,G})$. In characteristic $p > 0$, the vanishing of these local cohomology modules is related to the vanishing of those considered above by Peskine and Szpiro's vanishing theorem [32, Remarque p. 110].

Remark 4.12. It follows from the Hartshorne-Lichtenbaum vanishing theorem [21, Theorem 3.1] that $\mathrm{H}^{2d}_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) = 0$. This can also be deduced from Theorem 4.8. Indeed, the only potential element of the poset $\mathcal{S}_{V,G}$ of codimension $2d$ is $(1 \otimes 1)(V^G)$, and this occurs only if V^G is the origin. As $\mathcal{S}_{V,G}(>(1 \otimes 1)(V^G))$ is nonempty,

$$\widetilde{\mathrm{H}}_{-1}(\mathcal{S}_{V,G}(>(1 \otimes 1)(V^G)); \Bbbk) = 0\,,$$

and we are done.

4.4 Rigid reflection groups

In this section, we focus on rigid reflection groups. In this situation, every minimal reflecting subspace is a hyperplane, and in particular, the arrangement of reflecting subspaces $\mathcal{R}_{V,G}$ is a hyperplane arrangement. Recall that a simplicial complex is *pure* if each of its maximal facets has the same dimension. A pure simplicial complex is *shellable* if there is a linear ordering of its maximal facets (a *shelling*) $F_1, F_2, \ldots, F_t$ such that $F_i \cap \bigcup_{j<i} F_j$ is pure of codimension 1; we call a poset *shellable* if its order complex is pure and shellable. We use the following well-known technique in combinatorial topology; see, e.g., [44, Subsection 3.1].

Proposition 4.13. *The only nonvanishing homology of a shellable poset is in the dimension of the poset.*

We refer to [44, Subsection 3.2] for the notions and facts from poset topology used in the proof of the following result. This lemma is undoubtedly known, but we were unable

to find it in the literature in the form needed for the subsequent theorem.

Lemma 4.14. *If G acts on V as a rigid reflection group, and H is a reflecting hyperplane, then there exists a shelling of $\mathcal{R}_{V,G}$ starting with a facet containing H.*

Proof. Note first that it is equivalent to find such a shelling of the dual $\mathcal{R}^*_{V,G}$ of $\mathcal{R}_{V,G}$. Since $\mathcal{R}^*_{V,G}$ is the standard poset of a hyperplane arrangement, it is a geometric lattice, whose atoms are the reflecting hyperplanes. For any ordering of these atoms $H = H_1, H_2, \ldots, H_t$, label each edge of the Hasse diagram, (x, y), where y covers x, with the least integer i such that the join of x and H_i is y. This is an EL-labelling, so the associated lexicographic ordering on the maximal chains is a shelling, and the first facet of this shelling contains H. ∎

Theorem 4.15. *If G acts on V as a rigid reflection group, then the intersection poset of $\mathcal{S}_{V,G}$ is shellable.*

Proof. Order the elements of G

$$1 = \sigma_0 \ , \ \sigma_1 \ , \ \ldots \ , \ \sigma_{|G|-1}$$

so that for each $j > 0$ there is some $i < j$ such that $\sigma_i^{-1}\sigma_j$ is a reflection. We then construct a shelling inductively as follows.

First, by the identification $\mathcal{S}_{V,G}(\leqslant(1 \otimes 1)(W)) \cong \mathcal{R}_{V,G}$ from Lemma 4.5, list the facets in a shelling of $\mathcal{S}_{V,G}(\leqslant(1 \otimes 1)(V))$. Then, for $j > 0$, for a list of the facets of

$$\bigcup_{j'<j} \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_{j'})(V))$$

such that each subsequent facet intersects the union of the others in pure codimension 1, choose an $i < j$ such that $\sigma_i^{-1}\sigma_j$ is a reflection. By Lemmas 4.5 and 4.14, we may list the facets in a shelling of $\mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V))$ that starts with a facet F_j containing a facet of

$$\mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_i)(V)) \cap \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V)) \ = \ \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V^{\sigma_i^{-1}\sigma_j})) \, .$$

As this is a codimension 1 subposet of $\bigcup_{j'<j} \mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_{j'})(V))$, the facet F_j intersects the union of previously listed faces in codimension 1. Continue with the list of facets in the chosen shelling of $\mathcal{S}_{V,G}(\leqslant(1 \otimes \sigma_j)(V))$.

Iterating this procedure for all $j = 0, \ldots, |G| - 1$ produces a shelling of $\mathcal{S}_{V,G}$. ∎

As a consequence, we find that our method from Theorem 4.9 does not provide sharper bounds for rigid reflection groups.

Corollary 4.16. *If G acts on V as a d-dimensional rigid reflection group, then*

$$\mathrm{H}^t_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2]) = 0$$

for all $t \neq d$.

Proof. Since G is a rigid reflection group, G_W is a reflection group for each isotropy subgroup G_W. Then, by Theorem 4.15 and Proposition 4.13, we find that

$$\widetilde{\mathrm{H}}_i(\mathcal{S}_{V,G}(>(1\otimes 1)(V^{G_W}));\Bbbk) = 0 \quad \text{for all} \quad i \neq \operatorname{codim}(V^{G_W}) - 1\,.$$

Since

$$\mathcal{S}_{V,G}(>(1\otimes 1)(V^{G_W})) \cong \mathcal{S}_{V,G}(>(1\otimes \tau)(V^{G_W}))$$

for any τ, by Lemma 4.3, we have $\widetilde{\mathrm{H}}_i(\mathcal{S}_{V,G}(>p);\Bbbk) = 0$ for all $i \neq \operatorname{codim}(p) - 1$ and all p in the intersection poset. The result follows by Theorem 4.8. ∎

Conjecture 4.17. There exists a separating set of size d (that is, there exists a polynomial separating algebra) if and only if G is a rigid reflection group.

The following example shows that the bounds in Theorem 4.9 are not necessarily sharp if G is not a reflection group.

Example 4.18. Let G be the symmetric group on three letters, with elements

$$1\ ,\ (12) = \tau_3\ ,\ (13) = \tau_2\ ,\ (23) = \tau_1\ ,\ (132) = \sigma_1\ ,\ (123) = \sigma_2\,.$$

Let V be its standard three-dimensional permutation representation. Let $W = V^{\oplus n}$ with G acting diagonally. The group G acts on V as a rigid reflection group, and its action on W is as a rigid n-reflection group. Note that the intersection poset of $\mathcal{S}_{W,G}$ is isomorphic to that of $\mathcal{S}_{V,G}$, since for any subgroup H of G, one has $W^H = (V^H)^{\oplus n}$. This intersection poset is depicted in Figure 4.1 where gV is shorthand for $(1\otimes g)(V)$, and similarly for gV^h.

The complex of $\mathcal{S}_{V,G}(>(1\otimes 1)(V^G))$ is a graph, namely the subgraph of Figure 4.1 obtained by deleting the bottom vertex. Its homology may be computed by first contracting a maximal tree, depicted with solid lines; the resulting graph consists of the four dotted edges looped around a single point. We thus have

$$\widetilde{\mathrm{H}}_1(\mathcal{S}_{W,G}(>(1\otimes 1)(W^G));\Bbbk) \cong \widetilde{\mathrm{H}}_1(\mathcal{S}_{V,G}(>(1\otimes 1)(V^G));\Bbbk) \cong \Bbbk^4\,.$$

By Theorem 4.8, $\mathrm{H}^{5n-2}_{\mathcal{I}(\mathcal{S}_{W,G})}(\Bbbk[W^2]) \neq 0$, so, as in the argument of Theorem 4.9, we conclude that any separating set for W has at least $5n-2$ elements. Note that the bound provided by Theorem 4.9 for W is $4n-1$.

4.5 Examples of separating sets of minimal size

Below, we present a variety of examples of separating sets that realize the lower bound in Theorem 4.9, thereby showing that the bound is sharp for these actions and that the found separating sets are of minimal size. First, we review an example from Dufresne's thesis:

Proposition 4.19. ([15, Proposition 5.2.2]). *Let $G = \langle \sigma \rangle$ be the cyclic group of order m, and suppose $\Bbbk$ contain ζ, a primitive m^{th} root of unity. Let G act diagonally on $\Bbbk[V]$ by the rule*

$$\sigma(x_i) = \zeta^{d_i} x_i$$

where $1 = d_1 | d_2 | \cdots | d_n | m$. Then there is a separating set for $\Bbbk[V]^G$ of order $2n - 1$.

For this construction, a separating set of monomials $u_{i,j} : 1 \leqslant i \leqslant j \leqslant n$ is first identified; see [15, Proposition 5.2.2] for precise formulas for the $u_{i,j}$. The terms naturally align in a triangle. It is then shown that the values of the invariants $u_{i,j}$ can be recovered from the diagonal sums $S_k = \sum_{i+j=k} u_{i,j}$ of the triangle. This "triangle trick" is used in many of the examples below.

It is worth noting that Proposition 4.19 includes as a special case the m^{th} Veronese subring of a polynomial ring of dimension n, for $\text{char}(\Bbbk) \not| m$.

Here, we construct separating sets of minimal size for the indecomposable modular representations of a cyclic group of prime order, equal to the characteristic of the field $\Bbbk$. Our argument is greatly inspired by Sezer's iterative construction of a separating set (see [35]) and uses the triangle trick mentioned above. After an appropriate change of basis, any indecomposable representation of a cyclic group of prime order will be given by a Jordan block of size at most p. We may further choose a basis so that the action on the coordinate ring $\Bbbk[x_1, \ldots, x_n]$ with $n \leqslant p$ is as follows:

$$\begin{aligned} \sigma \cdot x_i &= x_i + x_{i+1}\,, \text{ for } i = 1, \ldots, n-1\,, \\ \sigma \cdot x_n &= x_n\,. \end{aligned}$$

One way to construct some invariants is to take norms (orbit products) and traces (orbit sums) of elements: in fact, by [31, Theorem 3], for representations of p-groups, norms and transfers will form a separating set. For $f \in \Bbbk[V]$, the *norm of f* is the orbit product $\mathrm{N}(f) := \prod_{i=0}^{p-1} (\sigma^i \cdot f)$ and the *trace of f* is the orbit sum $\mathrm{Tr}(f) := \sum_{i=0}^{p-1} (\sigma^i \cdot f)$.

Proposition 4.20. *Let V_n be the n-dimensional indecomposable representation of the cyclic group of order p. The set S_n of the sum of the elements appearing on the diagonal of the following triangle forms a separating set.*

$$\begin{array}{ccccccc} \mathrm{N}(x_1) & \mathrm{Tr}(x_1x_2^{p-1}) & \mathrm{Tr}(x_1x_3^{p-1}) & \cdots & \mathrm{Tr}(x_1x_{n-1}^{p-1}) & & \\ & \mathrm{N}(x_2) & \mathrm{Tr}(x_2x_3^{p-1}) & \cdots & \mathrm{Tr}(x_2x_{n-1}^{p-1}) & & \\ & & \mathrm{N}(x_3) & \ddots & \vdots & & \\ & & & & \mathrm{N}(x_{n-1}) & & \\ & & & & & x_n^p\,. & \end{array} \tag{4.3}$$

Proof. We proceed by induction on n. For $n = 2$, we have $\Bbbk[x_1, x_2]^{C_p} = \Bbbk[\mathrm{N}(x_1), x_2]$. As x_2 and x_2^p separate the same points, we are done.

Now, suppose $n \geqslant 2$. If $x_n^p = 0$, then $x_n = 0$ and the triangle (4.3) reduces to the triangle for V_{n-1}. Thus, the sum of the diagonals separate orbits by the induction hypothesis.

Now suppose that $x_n \neq 0$. For $i \geqslant n-2$, the coefficient of x_i in $\mathrm{Tr}(x_ix_{n-1}^{p-1})$ is

$$\begin{array}{l} x_{n-1}^{p-1} + \sum_{l=0}^{p-1} \binom{p-1}{j} x_{n-1}^j x_n^{p-1-j} \left(1 + 2^{p-1-j} + \cdots + (p-1)^{p-1-j}\right) \\ = x_{n-1}^{p-1} - x_n^{p-1} - x_{n-1}^{p-1} = -x_n^{p-1}. \end{array}$$

Indeed, in characteristic p, one has $\left(1 + 2^{p-1-j} + \ldots + (p-1)^{p-1-j}\right) = -1$ for $j = 0$ or $j = p-1$ and zero otherwise. It follows that

$$\Bbbk[x_1, \ldots, x_n, x_n^{-1}] = \Bbbk[\mathrm{Tr}(x_1x_{n-1}^{p-1}), \ldots, \mathrm{Tr}(x_{n-2}x_{n-1}^{p-1}), x_{n-1}, x_n, x_n^{-1}]\,.$$

Taking invariants, we then have:

$$\Bbbk[x_1, \ldots, x_n, x_n^{-1}]^{C_p} = \Bbbk[\mathrm{Tr}(x_1x_{n-1}^{p-1}), \ldots, \mathrm{Tr}(x_{n-2}x_{n-1}^{p-1}), \mathrm{N}(x_{n-1}), x_n, x_n^{-1}]\,.$$

Now we need only explain how to get these from S_n. The bottom two, $\mathrm{N}(x_{n-1})$ and $\mathrm{Tr}(x_{n-2}x_{n-1}^{p-1})$, are in S_n. As any term in the triangle can be expressed as a polynomial, up to dividing by a power of x_{n-1}, in elements of S_n lying either on the same row or below, we can express the remaining elements of S_n in terms of the sums of the diagonals. ∎

Let V_2 denote the two-dimensional indecomposable representation of C_p as above. We consider the diagonal representation of C_p on $V_2^{\oplus n}$. Let $x_1, y_1, \ldots, x_n, y_n$ be a choice of coordinates on $V_2^{\oplus n}$ such that $\sigma \cdot x_i = x_i$, and $\sigma \cdot y_i = x_i + y_i$. The ring of invariants is generated by

$$\begin{array}{ll} x_i\,, & 1 \leqslant i \leqslant n \\ u_{i,i} = \mathrm{N}(y_i) = y_i^p - x_i^{p-1}y_i\,, & 1 \leqslant i \leqslant n \\ u_{i,j} = x_iy_j - x_jy_i\,, & 1 \leqslant i < j \leqslant n \\ \mathrm{Tr}^{C_p}(y_1^{a_1} \cdots y_n^{a_n})\,, & a_i < p\,,\ \Sigma a_i \geqslant 2p-2\,. \end{array}$$

By [13, Corollary 3.9.14], the invariants of degree less than $|G| = p$ form a separating set: in particular, the generators

$$x_i : 1 \leqslant i \leqslant n \quad \text{and} \quad u_{ij} : 1 \leqslant i \leqslant j \leqslant n$$

form a separating set. Note that we have the relations

$$\begin{aligned} &x_i u_{j,k} - x_j u_{i,k} + x_k u_{i,j} && \forall i < j < k, \\ &x_i u_{j,j} - x_j u_{i,i} + x_i^{p-1} x_j^{p-1} u_{i,j} - u_{i,j}^p && \forall i < j\,. \end{aligned}$$

Set $S_\ell = \sum_{i+j=\ell} u_{i,j}$ for all $2 \leqslant \ell \leqslant 2n$. Remark that the S_ℓ correspond to the diagonal sums of the triangle consisting of the $u_{i,j}$.

Proposition 4.21. *The set of all x_i and S_ℓ is a separating set for $\Bbbk[V_2^{\oplus n}]^{C_p}$.*

Proof. It suffices to show that given the values of all x_i and f_ℓ, we may recover the values of each u_{ij}. We induce on n. If $n = 1$, there is nothing to show.

Case 1: $x_n \neq 0$: In this case, we may write

$$u_{i,i} = x_n^{-1}(x_i u_{n,n} + x_i^{p-1} x_n^{p-1} u_{i,n} + (-u_{i,n})^p\,) \tag{4.4}$$

$$u_{i,j} = x_n^{-1}(x_j u_{i,n} - x_i u_{j,n})\,, \qquad i < j \tag{4.5}$$

to express each $u_{i,j}$ with $j < n$ in terms of the x_s and $u_{k,n}$ with $k \geqslant j$. This enables us to express each $u_{i,j}$ in terms of the S_ℓ and x_s: indeed, $u_{n,n} = S_{2n}$, and if each $u_{i,j}$ with $j \geqslant k$ has such an expression, then

$$S_{n+k-1} = u_{k-1,n} + \sum_{\substack{i+j=n+k-1 \\ j \geqslant k}} u_{i,j}$$

provides such an expression for $u_{k-1,n}$, and the formulas (4.4) and (4.5) above provide such an expression for $u_{k-1,k-1}$ and each $u_{k-1,j}$.

Case 2: $x_n = 0$: Here, we have $y_n^p = u_{nn}$, so that $u_{i,n} = x_i y_n = x_i u_{n,n}^{1/p}$. Then, by the induction hypothesis, we may express each $u_{i,j}$ with $j < n$ in terms of the x_s and

$$\widehat{S}_\ell = \sum_{\substack{i+j=\ell \\ j<n}} u_{i,j} = S_\ell - x_{\ell-n} u_{n,n}^{1/p}$$

(where $x_{\ell-n} := 0$ for $\ell \leqslant n$), and thus in terms of the x_s and S_ℓ. ∎

As the action of C_p on $V_2^{\oplus n}$ is generated by n-reflections, by Theorem 4.9, any separating set for $\Bbbk[V_2^{\oplus n}]^{C_p}$ has at least $3n - 1$ elements. Thus, the set

$$\{x_i, S_\ell \mid 1 \leqslant i \leqslant n, 2 \leqslant \ell \leqslant 2n\}$$

is a separating set of minimal size.

Let $\Bbbk$ have characteristic 2 and G be the finite subgroup of $\mathrm{GL}_7(\mathbb{F}_2)$ given by

$$G := \left\{ \left(\begin{array}{cccc|c} & & I_4 & & \mathbf{0} \\ \hline \alpha_1 & 0 & 0 & \alpha_4 & \\ 0 & \alpha_2 & 0 & \alpha_4 & I_3 \\ 0 & 0 & \alpha_3 & \alpha_4 & \end{array} \right) \;\middle|\; \alpha_1, \ldots, \alpha_4 \in \mathbb{F}_2 \right\},$$

where I_m denotes the $m \times m$ identity matrix. The group G is isomorphic to C_2^4, and generated by reflections (namely those elements where exactly one of the α_i's is nonzero). This is a remarkable example since its invariant ring is not Cohen-Macaulay (see [27]) and, moreover, neither is any graded separating subalgebra (see [17]) despite the action of G being generated by reflections.

Setting all α_i's to be one yields an element σ whose fixed space of codimension 3 is a minimal reflecting subspace. By Theorem 4.9, it follows that any separating set contains at least 9 elements. Writing x_i for the coordinate functions on $V = \Bbbk^7$, one has the minimal generating set

$$\Bbbk[V]^G = \Bbbk[x_1, x_2, x_3, x_4, f_1, f_2, f_3, g_1, g_2, g_3, r]$$

where $\deg f_i = 3$, $\deg g_i = 4$, and $\deg r = 5$. Using a computer algebra system, one verifies that

$$f_i r \in \Bbbk[x_1, x_2, x_3, x_4, f_1, f_2, f_3, g_1, g_2, g_3], \text{ for } \quad i = 1, 2, 3, \tag{4.6}$$

$$r^2 \equiv (x_1 + x_4)^2 g_2 g_3 \mod (f_1, f_2, f_3)\,. \tag{4.7}$$

Thus, given the values of the x_i's, f_i's, and g_i's, one may recover the value of r using (4.6) if some $f_i \neq 0$ and (4.7) if all $f_i = 0$, so we can leave out r still have a separating set. One also finds

$$(x_3 + x_4) f_3 = f_2(x_2 + x_4) + f_1(x_1 + x_4) \tag{4.8}$$

$$(x_i + x_4)^2 g_3 \equiv f_i^2 \mod (x_3 + x_4), \quad i = 1, 2, \tag{4.9}$$

$$f_3 \equiv 0 \mod (x_1 + x_4, x_2 + x_4, x_3 + x_4)\,. \tag{4.10}$$

Hence, given the values of the x_i's, f_1, and f_2, one can either obtain the value of f_3 (using (4.8) if $x_3 \neq x_4$ or (4.10) if $x_1 = x_2 = x_3 = x_4$) or g_3 (using (4.9) if $x_3 = x_4$ and either $x_1 \neq x_4$ or $x_2 \neq x_4$). Concluding, we have the following.

Proposition 4.22. *The invariants $x_1, x_2, x_3, x_4, f_1, f_2, g_1, g_2, f_3 + g_3$ form a separating set for $\Bbbk[V]^G$ of minimal size.*

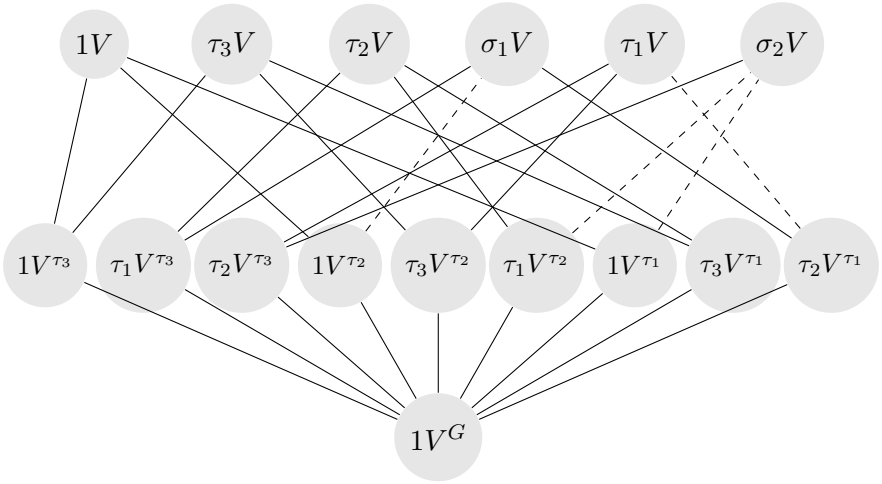


Figure 4.1. The intersection poset of the separating variety of the permutation representation of S_3.

CHAPTER 5

A QUESTION ON THE VANISHING OF LOCAL COHOMOLOGY

In this chapter, we pose a question on the vanishing of local cohomology with an application to invariant theory. Let R and S be graded domains with $R \subseteq S$, both finitely generated over a field $\Bbbk$. The ring $R \otimes_{\Bbbk} R$ is a subring of $S \otimes_{\Bbbk} S$, and both rings are domains. We note that if there is an R linear splitting ϕ of the inclusion of R into S, then $\phi \otimes_{\Bbbk} \phi$ is an $(R \otimes_{\Bbbk} R)$-linear splitting of the inclusion of $R \otimes_{\Bbbk} R$ into $S \otimes_{\Bbbk} S$.

Thus, given the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{1} & R \\ & {\scriptstyle i}\searrow \quad \nearrow{\scriptstyle \phi} & \\ & S & \end{array} ,$$

then the following diagram commutes

$$\begin{array}{ccc} R \otimes R & \xrightarrow{1} & R \otimes R \\ & {\scriptstyle i}\searrow \quad \nearrow{\scriptstyle \phi\otimes\phi} & \\ & S \otimes S & \end{array} . \tag{5.1}$$

For a domain A finitely generated graded domain, set

$$\Delta(A) = (a \otimes 1 - 1 \otimes a \,|\, a \in A) \subset A \otimes_{\Bbbk} A\,.$$

Applying a local cohomology functor, to diagram (5.1), the following commutes:

$$\begin{array}{ccc} \mathrm{H}^i_{\Delta(R)}(R \otimes R) & \xrightarrow{1} & \mathrm{H}^i_{\Delta(R)}(R \otimes R) \\ & {\scriptstyle i_*}\searrow \quad \nearrow{\scriptstyle (\phi\otimes\phi)_*} & \\ & \mathrm{H}^i_{\Delta(R)(S\otimes S)}(S \otimes S) & \end{array} . \tag{5.2}$$

In particular, if $\Bbbk[V]^G$ is a direct summand of $\Bbbk[V]$, the cohomological dimension of $\Delta(\Bbbk[V]^G)$ in $\Bbbk[V]^G \otimes \Bbbk[V]^G$ is less than or equal to the cohomological dimension of

$$\Delta(\Bbbk[V]^G)(\Bbbk[V^2]) = \mathcal{I}(\mathcal{S}_{V,G})$$

in the ring $\Bbbk[V^2]$.

Question 5.1. For which R as above is the cohomological dimension of $\Delta(R)$ equal to the dimension of R?

We note that Δ_R is a prime of height equal to the dimension of R, so this is a lower bound for the cohomological dimension. A sufficient condition for equality to hold is that R is a polynomial ring $R = \Bbbk[x_1, \dots, x_n]$, for then $\Delta(R) = (x_i \otimes 1 - 1 \otimes x_i \,|\, i = 1, \dots, n)$ is a complete intersection. The converse is not true in general, as the following example shows.

Example 5.2. Let $R = \overline{\mathbb{F}}_2[x^2, xy, y^2]$. Write $R \otimes R = \overline{\mathbb{F}}_2[x^2, xy, y^2, \bar{x}^2, \bar{x}\bar{y}, \bar{y}^2]$. Then

$$\Delta(R) = (x^2 - \bar{x}^2, xy - \bar{x}\bar{y}, y^2 - \bar{y}^2) \subseteq R \otimes R\,.$$

Now,

$$(xy - \bar{x}\bar{y})^2 = x^2y^2 - \bar{x}^2\bar{y}^2 = y^2(x^2 - \bar{x}^2) - \bar{x}^2(y^2 - \bar{y}^2) \in (x^2 - \bar{x}^2, y^2 - \bar{y}^2)\,,$$

so Δ_R is generated by two elements up to radical, and hence has cohomological dimension two.

We note that in the example above, R is a Veronese ring that is not a ring of invariants. If the Veronese subring is a ring of invariants, the vanishing above cannot occur.

Example 5.3. Let S be a polynomial ring in n variables over a field $\Bbbk$, and let $d \in \mathbb{N}$ be a unit in $\Bbbk$. Endow S with a $\mathbb{Z}/d\mathbb{Z}$-grading by taking the standard grading modulo d. Then $S \otimes S$ has a $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z})$-grading coming from the $\mathbb{Z}/d\mathbb{Z}$-grading on each factor. Note that there is a retraction $S \otimes S \to S^{(d)} \otimes S^{(d)}$ given by taking the $(0,0)$-degree piece.

One may compute $\mathrm{H}^i_{\Delta(S^{(d)})}(S^{(d)} \otimes S^{(d)})$ by taking cohomology of a Čech complex on the generating set

$$\{m \otimes 1 - 1 \otimes m \,|\, m \text{ is a monomial in } S \text{ of degree } d\}\,,$$

with coefficients in $S^{(d)} \otimes S^{(d)}$. This generating set is homogeneous with respect to the $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z})$-grading. Thus, one may take a Čech complex on the same generating set with coefficients in $S \otimes S$, take cohomology, and then pass to the $(0,0)$-degree piece, and one will obtain the same modules. That is,

$$\mathrm{H}^i_{\Delta(S^{(d)})}(S^{(d)} \otimes S^{(d)}) = \rho\big(\mathrm{H}^i_{\Delta(S^{(d)})(S \otimes S)}(S \otimes S)\big)\,,$$

where ρ denotes the $(0,0)$-degree piece in the $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z})$-grading. Now, the ideal $\Delta(S^{(d)})(S \otimes S)$ is the separating ideal of the scalar action defining the Veronese subring,

hence by Lemma 4.3, its variety is the union of d subspaces of dimension n inside affine $2n$-space. By Theorem 4.9, the $2n-1$ local cohomology of $S \otimes S$ with support in this ideal is nonzero. At any point other than the origin, this variety is locally equal to an n-dimensional subspace, so

$$\mathrm{H}^{2n-1}_{\Delta(S^{(d)})(S\otimes S)}(S \otimes S)$$

is supported on the maximal ideal and hence isomorphic to a graded shift of a direct sum of copies of the injective hull E of $\Bbbk$ over $S \otimes S$. Now, with respect to the $(\mathbb{Z} \times \mathbb{Z})$-grading on $S \otimes S$ induced by the standard grading on S, $E \cong \underline{\mathrm{Hom}}_{S\otimes S}(S \otimes S, \Bbbk)$ is nonzero in all degrees (a, b) with $a, b \leqslant 0$. Thus, this cohomology module is nonzero in all degrees in the $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z})$-grading. Therefore,

$$\mathrm{H}^{2n-1}_{\Delta(S^{(d)})}(S^{(d)} \otimes S^{(d)}) = \rho\big(\mathrm{H}^{2n-1}_{\Delta(S^{(d)})(S\otimes S)}(S \otimes S)\big) \neq 0\,.$$

Motivated by the above examples, we ask the following variant of Question 5.1:

Question 5.4. Let $G \leq \mathrm{GL}(V)$ be finite and suppose that for $i > \dim(V)$,

$$\mathrm{H}^{i}_{\Delta(\Bbbk[V]^G)}(\Bbbk[V]^G \otimes \Bbbk[V]^G) = 0\,.$$

Is $\Bbbk[V]^G$ then regular?

We note that the hypothesis of the above question does not depend at all on G, except that $\Bbbk[V]^G$ is the ring of invariants of some finite group action. A positive answer to Question 5.4 has an interesting consequence.

If G is a rigid reflection group and $\Bbbk[V]^G$ is F-regular, then $\mathrm{H}^{i}_{\Delta(\Bbbk[V]^G)}(\Bbbk[V]^G \otimes \Bbbk[V]^G)$ injects into $\mathrm{H}^{i}_{\mathcal{I}(\mathcal{S}_{V,G})}(\Bbbk[V^2])$, which vanishes for all $i > \dim(V)$ by Corollary 4.16. Thus, if Question 5.4 is true, then if G is a rigid reflection group and $\Bbbk[V]^G$ is F-regular, then $\Bbbk[V]^G$ is a polynomial ring.

REFERENCES

[1] I. M. Aberbach and G. J. Leuschke, *The F-signature and strong F-regularity*, Math. Res. Lett., 10 (2003), pp. 51–56.

[2] J. Àlvarez Montaner, R. García López, and S. Zarzuela Armengou, *Local cohomology, arrangements of subspaces and monomial ideals*, Adv. Math., 174 (2003), pp. 35–56.

[3] M. Auslander, *On the purity of the branch locus*, Amer. J. Math., 84 (1962), pp. 116–125.

[4] D. J. Benson, *Polynomial invariants of finite groups*, vol. 190 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 1993.

[5] M.-J. Bertin, *Anneaux d'invariants d'anneaux de polynomes, en caractéristique p*, C. R. Acad. Sci. Paris Sér. A-B, 264 (1967), pp. A653–A656.

[6] A. Broer, *The direct summand property in modular invariant theory*, Transform. Groups, 10 (2005), pp. 5–27.

[7] ——, *On Chevalley-Shephard-Todd's theorem in positive characteristic*, in Symmetry and spaces, vol. 278 of Progr. Math., Birkhäuser Boston, Inc., Boston, MA, 2010, pp. 21–34.

[8] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, vol. 39 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1993.

[9] H. E. A. Campbell, I. P. Hughes, and R. J. Shank, *Preliminary notes on rigid reflection groups*. Preprint.

[10] J. Chan, *Integer torsion in local cohomology, and questions on tight closure theory*, ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.)–The University of Utah.

[11] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math., 77 (1955), pp. 778–782.

[12] A. Clark and J. Ewing, *The realization of polynomial algebras as cohomology rings*, Pacific J. Math., 50 (1974), pp. 425–434.

[13] H. Derksen and G. Kemper, *Computational invariant theory*, Invariant theory and algebraic transformation groups, I, Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[14] J. Draisma, G. Kemper, and D. Wehlau, *Polarization of separating invariants*, Canad. J. Math., 60 (2008), pp. 556–571.

[15] E. Dufresne, *Separating invariants*, ProQuest LLC, Ann Arbor, MI, 2008. Thesis (Ph.D.)–Queen's University (Canada).

[16] ——, *Separating invariants and finite reflection groups*, Adv. Math., 221 (2009), pp. 1979–1989.

[17] E. Dufresne, J. Elmer, and M. Kohls, *The Cohen-Macaulay property of separating invariants of finite groups*, Transform. Groups, 14 (2009), pp. 771–785.

[18] E. Dufresne and J. Jeffries, *Separating invariants and local cohomology*, Adv. Math., 270 (2015), pp. 565–581.

[19] D. Glassbrenner, *The Cohen-Macaulay property and F-rationality in certain rings of invariants*, J. Algebra, 176 (1995), pp. 824–860.

[20] A. Grothendieck, *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux* (*SGA* 2), North-Holland Publishing Co., Amsterdam; Masson & Cie, Éditeur, Paris, 1968. Augmenté d'un exposé par Michèle Raynaud, Séminaire de Géométrie Algébrique du Bois-Marie, 1962, Advanced Studies in Pure Mathematics, Vol. 2.

[21] R. Hartshorne, *Cohomological dimension of algebraic varieties*, Ann. of Math. (2), 88 (1968), pp. 403–450.

[22] M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math., 93 (1971), pp. 1020–1058.

[23] M. Hochster and C. Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math. Soc., 3 (1990), pp. 31–116.

[24] C. Huneke and G. J. Leuschke, *Two theorems about maximal Cohen-Macaulay modules*, Math. Ann., 324 (2002), pp. 391–404.

[25] S. B. Iyengar, G. J. Leuschke, A. Leykin, C. Miller, E. Miller, A. K. Singh, and U. Walther, *Twenty-four hours of local cohomology*, vol. 87 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2007.

[26] V. Kac and K. Watanabe, *Finite linear groups whose ring of invariants is a complete intersection*, Bull. Amer. Math. Soc. (N.S.), 6 (1982), pp. 221–223.

[27] G. Kemper, *On the Cohen-Macaulay property of modular invariant rings*, J. Algebra, 215 (1999), pp. 330–351.

[28] ——, *Loci in quotients by finite groups, pointwise stabilizers and the Buchsbaum property*, J. Reine Angew. Math., 547 (2002), pp. 69–96.

[29] ——, *Computing invariants of reductive groups in positive characteristic*, Transform. Groups, 8 (2003), pp. 159–176.

[30] G. Lyubeznik, *On some local cohomology modules*, Adv. Math., 213 (2007), pp. 621–643.

[31] M. D. Neusel and M. Sezer, *Separating invariants for modular p-groups and groups acting diagonally*, Math. Res. Lett., 16 (2009), pp. 1029–1036.

[32] C. Peskine and L. Szpiro, *Dimension projective finie et cohomologie locale. Applications à la démonstration de conjectures de M. Auslander, H. Bass et A. Grothendieck*, Inst. Hautes Études Sci. Publ. Math., (1973), pp. 47–119.

[33] F. Reimers, *Polynomial separating algebras and reflection groups*, arXiv preprint arXiv:1307.7522, (2013).

[34] J.-P. Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, in Colloque d'Algèbre (Paris, 1967), Exp. 8, Secrétariat mathématique, Paris, 1968, pp. 1–11.

[35] M. Sezer, *Explicit separating invariants for cyclic P-groups*, J. Combin. Theory Ser. A, 118 (2011), pp. 681–689.

[36] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math., 6 (1954), pp. 274–304.

[37] A. K. Singh, *Failure of F-purity and F-regularity in certain rings of invariants*, Illinois J. Math., 42 (1998), pp. 441–448.

[38] ——, *The F-signature of an affine semigroup ring*, J. Pure Appl. Algebra, 196 (2005), pp. 313–321.

[39] K. E. Smith and M. Van den Bergh, *Simplicity of rings of differential operators in prime characteristic*, Proc. London Math. Soc. (3), 75 (1997), pp. 32–62.

[40] L. Smith, *On alternating invariants and Hilbert ideals*, J. Algebra, 280 (2004), pp. 488–499.

[41] R. P. Stanley, *Eulerian partitions of a unit hypercube*, Higher Combinatorics (M. Aigner, ed.), Reidel, Dordrecht/Boston, 49 (1977).

[42] K. Tucker, *F-signature exists*, Invent. Math., 190 (2012), pp. 743–765.

[43] M. R. Von Korff, *The F-Signature of Toric Varieties*, ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–University of Michigan.

[44] M. L. Wachs, *Poset topology: tools and applications*, in Geometric combinatorics, vol. 13 of IAS/Park City Math. Ser., Amer. Math. Soc., Providence, RI, 2007, pp. 497–615.

[45] K.-i. Watanabe and K.-i. Yoshida, *Minimal relative Hilbert-Kunz multiplicity*, Illinois J. Math., 48 (2004), pp. 273–294.